

**Wet van 30 juli 2018 betreffende
de bescherming van natuurlijke
personen met betrekking tot de
verwerking van
persoonsgegevens**

Evaluatierapport

2021

Mathieu MICHEL
Staatssecretaris voor Privacy

VOORWOORD



Van bij de aanvang van mijn mandaat als staatssecretaris voor Privacy heb ik het belang onderstreept van het vertrouwen van de burger in de verwerking van zijn persoonsgegevens in volledige overeenstemming met de Europese en nationale regelgeving. De ontwikkeling en de toepassing van nieuwe technologieën en de digitale transformatie van onze samenleving berusten immers in grote mate op het verwerken van data.

Ook de maatregelen die we in het kader van de strijd tegen de pandemie hebben moeten treffen en de verwerking van persoonsgegevens die daarmee gepaard gaan hebben nogmaals het belang aangetoond van een

solide en duidelijk reglementair kader op grond waarvan transparante gegevensstromen tot stand kunnen komen en privacyvriendelijke digitale applicaties kunnen worden ontwikkeld.

De wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens schrijft een evaluatie van de wet voor die in 2021 moet plaatsvinden. Ik kan uiteraard de Privacywet niet evalueren zonder voeling te hebben met de toepassing van de wet door de betrokken actoren op het terrein, met name de verwerkingsverantwoordelijken, de verwerkers, de gegevensbeschermingsfunctionarissen maar even goed de burger, het maatschappelijk middenveld, de vakbonden, professionele organisaties en vele anderen die dagelijks instaan voor het verwerken van data en de rechten en verplichtingen van de Privacywet toepassen.

Gelet op de uitdagingen waar we vandaag voor staan om het vertrouwen van de burger in de verwerking van zijn gegevens te versterken heb ik mij echter niet beperkt tot een evaluatie van de letter van de Privacywet. De digitale samenleving evolueert snel. Ik heb de evaluatie dan ook willen voeden met een bredere reflectie over de verhouding tussen privacy, innovatie en digitale transformatie.

De evaluatie is uitgemond in dit rapport met aanbevelingen die ik aan de Kamer van volksvertegenwoordigers zal voorstellen. Met deze aanbevelingen in de hand beschik ik over een rijke waaier aan oriënteringen om het reglementaire kader van de gegevensbescherming verder aan te vullen en te versterken, de gegevensstromen op meer transparante wijze te kunnen organiseren en het institutionele landschap van de toezichthoudende autoriteiten bij te sturen.

Ik wil iedereen bedanken die bijgedragen heeft tot deze evaluatie. De Privacywet is onbetwistbaar een essentieel reglementair kader voor de digitale transformatie die deze regering ambieert. Het vertrouwen in de verwerking van onze persoonsgegevens moet daarbij centraal staan.

Mathieu MICHEL

Staatssecretaris voor Privacy

1. INLEIDING

De Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (hierna « Privacywet ») legt een evaluatie van de wet op in de loop van het derde jaar na de inwerkingtreding ervan, in 2021 dus.

Deze evaluatie vindt plaats drie jaar na de inwerkingtreding van ook de Algemene Verordening Gegevensbescherming¹ (hierna « AVG ») en van de omzetting van de Europese Richtlijn betreffende de verwerking van persoonsgegevens door handhavingsautoriteiten (hierna « de Richtlijn »)². Tot slot heeft de Privacywet ook een wettelijk kader gecreëerd voor de verwerking van persoonsgegevens door overheidsdiensten die buiten de bevoegdheidssfeer van de Europese Unie vallen, met name de inlichtingendiensten.

Op Belgisch niveau werd destijds dus gekozen voor dit allesomvattend wettelijk kader voor de bescherming van persoonsgegevens om te voorkomen dat de toepassing en omzetting van de Europese wetgeving gefragmenteerd zou gebeuren. Dit maakt dat de evaluatie van de Privacywet een zeer omvangrijke oefening is die raakt aan een brede waaier aan belanghebbenden. Gegevens zijn immers zowel de motor als de olie van de hedendaagse digitale modernisering. Gaat het nu om het organiseren van een efficiënte en toegankelijke dienstverlening door onze administratieve overheden of om het ontwikkelen van de nieuwste technologische toepassingen in allerlei domeinen van onze samenleving, de persoonsgegevens van de burger liggen er aan de basis van.

De omwenteling die er in 2018 vooral met de AVG heeft plaatsgevonden heeft de nodige commotie veroorzaakt. Het heeft veel vragen doen rijzen naar de concrete toepassing van deze vernieuwde privacystandaarden en naar de mogelijke gevolgen in geval van niet-naleving ervan. De Europese Unie heeft de lat voor de bescherming van onze persoonsgegevens immers hoog gelegd en iedereen moet over die lat heen kunnen. Vandaag, meer dan drie jaar na de inwerkingtreding, stellen we vast dat dit nog altijd geen evidentie is, zowel voor diegene die verplichtingen moeten naleven als voor de controleautoriteiten die hierop moeten toezien.

Met de evaluatie van de Privacywet heeft de wetgever aan het beleidsniveau de kans geboden om kort op de bal te spelen. In de eerste plaats kan gepeild worden naar de impact van de nieuwe wetgeving. De aanpassing aan de vernieuwde standaarden heeft een ernstige inspanning gevergd van alle betrokkenen. Dit evaluatierapport kan dienen als vertrekpunt om het beleid bij te sturen. Waar dit noodzakelijk wordt geacht en voor zover het toepasselijke Europees recht daartoe de mogelijkheid biedt zal de evaluatie dan ook aanleiding geven tot de nodige wettelijke aanpassingen en beleidsmaatregelen.

Daarnaast biedt deze evaluatie ook de mogelijkheid om een bredere reflectie en een inhoudelijk debat te voeren over het belang dat moet gehecht worden aan privacy in onze samenleving. In welke verhouding staat de bescherming van de persoonlijke levenssfeer tot andere grondrechten en hoe kan

¹ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, PB L 119 van 4 mei 2016, blz. 1-88.

² Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, PB L 119 van 4 mei 2016, blz. 89-131

innovatie en digitale transformatie verenigd worden met een robuuste bescherming van onze persoonsgegevens ? De bescherming van persoonsgegevens staat onbetwistbaar centraal in deze evaluatie. Vaak wordt echter vergeten dat de AVG evengoed het vrije verkeer van gegevens wenst te bevorderen, getuige hiervan bijvoorbeeld het recht op overdraagbaarheid van persoonsgegevens of de principes inzake de doorgifte van gegevens voor verenigbare of verdere verwerking.

Naast de Privacywet raakt deze evaluatie dan ook onvermijdelijk aan aanverwante wetgeving en maatregelen die aan de basis liggen van een werkelijk databeheerbeleid. De conclusies en aanbevelingen in dit rapport vormen dan ook een mogelijke blauwdruk om de doorstroming te faciliteren van persoonsgegevens binnen de overheidssector, tussen verschillende overheidsniveaus en tussen de publieke en private sector.

Tot slot is een evaluatie van het materiële privacyrecht onlosmakelijk verbonden met het institutionele privacylandschap. Enerzijds spelen meerdere instellingen een rol bij het faciliteren van de doorstroming van data. Anderzijds heeft de Belgische wetgever er in 2018 ook voor gekozen om op federaal niveau vier toezichthoudende aan te stellen. Daarnaast moet ook rekening gehouden worden met deelstatelijke toezichthoudende autoriteiten en dienstenintegratoren. Dit maakt het institutionele privacylandschap bijzonder complex hetgeen de doorstroming van data of het toezicht op het respecteren van de wetgeving niet noodzakelijk faciliteert. Ook deze dimensie is dus een bijzonder aandachtspunt doorheen deze evaluatie en kan aanleiding geven tot een aanpassing van het institutionele landschap.

2. METHODOLOGIE GEHANTEERD VOOR DE EVALUATIE VAN DE PRIVACYWET

De evaluatie van de Privacywet heeft plaatsgevonden tussen februari en september 2021 en werd gevoerd aan de hand van een uitgebreide raadpleging van en dialoog met geïnteresseerde en betrokken belanghebbenden.

Organisatorisch werd in de eerste plaats **een begeleidingscomité** opgericht bestaande uit vier academische privacyexperten om de oefening in goede banen te leiden:

- Paul DE HERT (VUB)
- Willem DEBEUCKELAERE (UGent)
- David RESTREPO AMARILES (ULB)
- Jean-Marc VAN GYSEGHEM (Unamur)

Dit begeleidingscomité werd aangesteld met als mandaat advies te verlenen aangaande het proces van de evaluatie en de te hanteren methodologie, deel te nemen aan hoorzittingen met belanghebbenden en de bijdragen van de geraadpleegde betrokkenen te analyseren. Het is belangrijk te benadrukken dat het evaluatierapport geen wetenschappelijk rapport is onderschreven en aangenomen door de leden van het begeleidingscomité. Zij boden net als de Dienst Privacy van de FOD Justitie en het Directoraat-Generaal Digitale Transformatie van de FOD BOSA een ondersteunende rol in het opstellen van het rapport.

Inhoudelijk vervolgens, is het gelet op de transversale impact van een reglementering zoals die betreffende de bescherming van persoonsgegevens de bedoeling geweest om een zo groot mogelijke diversiteit aan belanghebbenden de kans te geven om hun mening, ervaring en visie te delen. De

interesse in de evaluatie is groot gebleken en heeft meer dan veertig bijdragen opgeleverd van autoriteiten, ondernemingen, beroepsverenigingen, academici, organisaties en burgers.

Een **grootschalige raadpleging** werd georganiseerd rond drie centrale vraagstellingen :

- wat zijn de sterktes en de tekortkomingen in de huidige Privacywet ?
- hoe kunnen we rond het gebruik van persoonsgegevens het vertrouwen versterken en de transparantie vergroten ?
- hoe kunnen we innovatie, die steunt op gegevensverzameling, stimuleren en tegelijk verzoenen met de nood aan een solide reglementair kader dat rechtszekerheid kan bieden ?

Op 17 juni heeft een **Webinar** plaatsgevonden met de titel « Voldoet de Privacywet aan de behoeften van onze samenleving ? » waaraan 390 personen hebben deelgenomen. Tegelijk was het Webinar ook het startschot voor een brede **publieke online raadpleging**. In het verlengde van de Webinar en de publieke raadpleging werden ook drie **thematische sessies** georganiseerd :

Sessie A : De toepassingsinstrumenten van de Privacywet

-  Gedragscodes/Certificering/Best practices/Sandboxes/Privacy ruling
-  Gegevensbeschermingsanalyses (DPIA)
-  Privacy by design/Privacy by default
-  Het delen van gegevens/hergebruiken van persoonsgegevens

Sessie B : Communicatie & sensibilisering

-  Informatie en begeleiding
-  Transparantie : gegevensverwerkingsregister, publicatie DPIA, publicatie beslissingen van de toezichthoudende autoriteiten in het Belgisch Staatsblad
-  Rechten van de betrokkenen : recht op vergetelheid, overdraagbaarheid van gegevens, identificeren van problemen in de uitoefening van de rechten
-  Rol van de gegevensbeschermingsfunctionaris

Sessie C : de verwerking van gegevens voor wetenschappelijk of historisch onderzoek, archivering of statistieken

-  Anonimisering en pseudonisering van persoonsgegevens
-  Veiligheidsmaatregelen
-  Verwerken van gevoelige persoonsgegevens
-  Het verspreiden/hergebruiken van persoonsgegevens of onderzoeksresultaten
-  Toegang tot persoonsgegevens
-  Uitoefenen van de rechten van de betrokkenen

Een evaluatie van de Privacywet kan ook niet plaatsvinden zonder de kritische blik van de **toezichthoudende autoriteiten** die door de wetgever zijn gemandateerd om de uitvoering ervan te begeleiden en het niet naleven te sanctioneren. De toepassing van de AVG en de Privacywet sinds 2018 levert belangrijke inzichten op in hoofdte van deze toezichthoudende autoriteiten en in het bijzonder wat hun eigen functioneren betreft en de verhoudingen tot elkaar. Een dialoog heeft dan ook plaatsgevonden met elk van de toezichthoudende autoriteiten teneinde hen de mogelijkheid te geven

hun opmerkingen en aanbevelingen toe te lichten en te bespreken.

Tot slot, het evaluatierapport geeft in deel 3 een feitelijke weerslag van alle bijdragen die ofwel op verzoek ofwel spontaan werden aangebracht. De inhoud van deel 3 is dan ook op geen enkele wijze een weerspiegeling van enig regeringsstandpunt. Dit werd voorbehouden voor deel 4 waarin op basis van de bijdragen van de belanghebbenden een aantal conclusies, aanbevelingen en suggesties voor verdere werkzaamheden worden samengevat.

3. EVALUATIE VAN DE PRIVACYWET DOOR ALLE DEELNEMENDE BELANGHEBBENDEN

3.1. Het wettelijk kader voor gegevensverwerking en rechtszekerheid

De keuze voor een kaderwet Privacy. Op Belgisch niveau werd in 2018 gekozen voor een allesomvattend wettelijk kader voor de bescherming van persoonsgegevens. Deze aanpak wordt nog steeds toegejuicht maar de Privacywet heeft daardoor ook aan helderheid en leesbaarheid ingeboet omwille van de bruggen die dienden te worden geslaan tussen verschillende beschermingsregimes. Anderzijds bestaat er ook tal van sectorale wetgeving die specifieke bepalingen bevatten betreffende de bescherming van persoonsgegevens maar die sinds de inwerkingtreding van de AVG nog niet zijn geactualiseerd.

Daarnaast is er sprake van een fragmentering van het institutionele landschap zowel door de veelheid aan toezichthoudende autoriteiten en intermediaire entiteiten die toegang verschaffen tot persoonsgegevens als door de verspreiding van het organieke wettelijke kader van deze autoriteiten en entiteiten. Er dringt zich met andere woorden een rationalisering en harmonisering van de wetgeving op zowel op het vlak van het materieel recht als wat betreft de bevoegde autoriteiten en entiteiten.

Transparantie en verantwoordelijkheid ('accountability') zijn beginselen die centraal staan in het gegevensbeschermingsrecht en dat moet ook weerspiegeld worden in de toepasselijke reglementering. Een privacywet moet in toegankelijke, begrijpbare en duidelijke taal te worden opgesteld zodat iedereen, niet alleen de specialisten maar bovenal de burger, kan begrijpen welke de mogelijkheden en de grenzen zijn van wat er met zijn of haar persoonsgegevens kan gebeuren.

Verantwoordelijkheid en bewustwording. Het bewustzijn over gegevensbescherming is aanzienlijk verhoogd sinds de komst van de AVG en de Privacywet. De besturen gaan meer doordacht om met de verwerking van gegevens en de bijhorende privacyaspecten. Ook privéorganisaties werden met de komst van de nieuwe wetgeving aangemoedigd om adequate beveiligingsmaatregelen in te voeren. De sancties die intussen door de Gegevensbeschermingsautoriteit zijn opgelegd bij verschillende inbreuken van de wetgeving hebben eveneens bijgedragen tot een grotere responsabilisering van verwerkingsverantwoordelijken. Ook de bewustwording bij de consumenten die steeds meer kiezen voor privacyvriendelijke toepassingen en bedrijven maakt dat privéorganisaties toenemend inzetten op privacybescherming en dit beschouwen als een concurrentieel voordeel.

Anderzijds wordt er ook op gewezen dat er niet enkel verplichtingen bestaan in hoofde van de verwerkingsverantwoordelijken. Ook de burger speelt een belangrijke rol in de bescherming van zijn

eigen persoonsgegevens. Geïnformeerd en bewust omgaan met de eigen data draagt evengoed bij tot een samenleving waarin op een positieve manier de privacy van eenieder en door eenieder wordt gerespecteerd en bevorderd.

Lacunes in de huidige Privacywet. Meerdere instanties hebben aangegeven dat er nood is aan verduidelijking van bepaalde concepten of terminologieën zoals ‘een persoonsgegeven’, de ‘uitoefening van gerechtelijke taken’, ‘doorgifte van persoonsgegevens’, ‘gezondheidsgegevens’, ‘diensten van de informatiemaatschappij’, ‘wetenschappelijk onderzoek’, ‘anonimisering’, het begrip ‘overheidsinstantie’ of de notie ‘verwerkingsverantwoordelijke’. Sommige van deze bepalingen worden onvoldoende of te vaag gedefinieerd,

andere worden niet gedefinieerd. In ieder geval geeft dit aanleiding tot verschillende of afwijkende interpretaties en dus toepassingen. In het bijzonder de kwalificering van vzw’s als een overheid omdat hun activiteiten in hoofdzaak door overheden of publieke instellingen worden gefinancierd of hun beheer onderworpen is aan toezicht door deze overheden of instellingen (cfr. artikel 5, 3° Privacywet) wordt in vraag gesteld door de non-profit sector. Deze kwalificering brengt immers administratieve en financiële verplichtingen mee die vaak moeilijk kunnen gedragen worden door de vzw’s. De aanstelling van een gegevensbeschermingsfunctionaris is bijvoorbeeld een bijkomende last die moeilijk te verantwoorden zou zijn voor kleine organisaties met beperkte middelen. Naar analogie van de Luxemburgse wetgeving zou een criterium kunnen gehanteerd worden volgens dewelke verenigingen die slechts bijkomstig aan gegevensverwerking doen niet onder de verplichting vallen een gegevensbeschermingsfunctionaris aan te moeten duiden.

Ook de draagwijdte van bepaalde artikelen in de Privacywet zou kunnen verduidelijkt worden, bijvoorbeeld de specifieke regels die voorzien zijn in hoofdstuk IV van Titel 1 voor de publieke sector. Ook is meer duiding nodig bij de invulling van bepaalde verplichtingen die door de Privacywet worden opgelegd, bijvoorbeeld de waarborgen bij de verwerking van bijzondere gegevenscategorieën overeenkomstig de artikel 9 en 10 van de Privacywet.

Er wordt ook onderlijnd dat er nood is aan een duidelijker rechtskader voor internationale gegevensuitwisselingen, bijv. voor gebruik van clouddiensten. Zowel op regelgevend als op praktisch vlak dient nauwer samengewerkt te worden tussen nationale en internationale regelgevende instanties, bijvoorbeeld door de ontwikkeling van een concreet rechtskader inzake wederzijdse bijstand. Er wordt ook de vraag gesteld naar het bestaan van voldoende informatie over en begrip van ontwikkelingen met betrekking tot internationale gegevensdoorgiften. Dit wordt aangestipt als één van de belangrijkste reglementaire belemmeringen voor innovatie. De rechtspraak Schrems II van het Europees Hof van Luxemburg heeft verregaande gevolgen voor internationale gegevensdoorgiften en de wijze waarop ondernemingen hiermee moeten omgaan. Dit veroorzaakt vertragingen en moeilijkheden in contractonderhandelingen. In het bijzonder KMO’s zijn niet uitgerust met de middelen en kennis om aan de strenge vereisten van het Europees Hof te voldoen.

“Privacy is een maatschappelijke uitdaging geworden. Het is verbonden met de maatschappelijke verantwoordelijkheid. Elke burger heeft recht op toegang tot digitalisering zonder dat de gegevens die hij in ruil voor een dienst of product verstrekt, in het gedrang komen. De pandemie heeft ons in een paar maanden naar een nieuwe dimensie gestuwd. De meeste burgers zijn er gewoon niet op voorbereid en zijn zich al helemaal niet bewust van de risico's die aan digitalisering verbonden zijn. Op mijn niveau probeer ik privacy te integreren in de bedrijfsverantwoordelijkheid, het jaarverslag en de bedrijfsstrategie.” (een gegevensbeschermingsfunctionaris)

De Privacywet moet ook meer duidelijkheid verschaffen over de bruggen tussen de verschillende onderdelen van de wet. Zoals eerder vermeld betreft het een allesomvattend wettelijk kader dat de gegevensbeschermingsregimes van meerdere types van autoriteiten en gegevensverwerkingen bepaalt. Dit weerspiegelt onder meer het bestaan van ook een onderscheid op Europees niveau tussen de AVG en de Richtlijn enerzijds en tussen het recht van de Europese Unie en de gegevensbeschermingsregimes die niet hun oorsprong kennen in het Europees recht anderzijds. Er is echter nood aan een verduidelijking van de grenzen tussen de verschillende gegevensbeschermingsregimes zodat de bepaling van de verwerkingsverantwoordelijke, de bijhorende verplichtingen en de correcte rechtsgrond voor de gegevensverwerking kan worden vastgesteld.

In dat opzicht stelt zich de vraag in welke mate er zich een herziening opdringt van de oplistings van de autoriteiten die overeenkomstig artikel 26, 7° binnen het bevoegdheidsdomein van Titel 2 van de Privacywet vallen. Dienen bepaalde autoriteiten zoals het gevangeniswezen toegevoegd te worden of volstaat het de scheidingslijn tussen de gegevensbeschermingsregimes te verduidelijken? De politievragen of het strafregister zijn bijvoorbeeld vragende partij voor dit laatste. Zij worden immers geconfronteerd met de mogelijkheid van een verkeerde toepassing of interpretatie van de regelgeving hetgeen op zijn beurt verregaande gevolgen heeft voor de uitoefening van de rechten van de betrokkenen.

Ook wordt gesuggereerd een betere opdeling te maken langs de lijnen van een algemeen toepassingsgebied enerzijds en de bijzondere gegevensbeschermingsregimes anderzijds. Sommige openbare diensten zijn belast met gegevensverwerkingen die mogelijks onder meerdere privacybeschermingsregimes vallen, in het bijzonder de autoriteiten in de veiligheidssector. Naast de AVG zijn daarbij vaak de Titels 2 of 3 van de Privacywet alsook bijzondere wetgeving van toepassing. Dit maakt een correcte toepassing van het rechtskader complex en moeilijk uit te leggen naar de burger toe. Hetzelfde geldt voor de verplichting van het sluiten van protocollen in het kader van gegevensuitwisselingen (cfr. artikel 20 Privacywet). Er bestaat onduidelijkheid over de toepassing van deze verplichting wanneer het gegevensverwerkingen betreft die onder meerdere privacybeschermingsregimes vallen.

Er wordt ook gesuggereerd om een debat te houden over de verplichtingen inzake het bewaren van persoonsgegevens, zowel wat betreft het territoriaal bepalen van de bewaringsplicht (regionaal, nationaal, Europees) als de technische specificaties en standaarden voor de bewaring (bijvoorbeeld gecentraliseerd of gedecentraliseerd). Bovendien bestaat er ook onduidelijkheid over de toe te passen bewaartermijnen. Vaak zijn de termijnen vaag of niet bepaald of zijn ze verspreid in verschillende regelgevingen. Bovendien zijn bepaalde bewaartermijnen die wettelijk opgelegd worden niet in overeenstemming met andere geldende wettelijke bepalingen. Dit is bijvoorbeeld het geval in de financiële sector. Verwerkingsverantwoordelijken zouden gebaat zijn bij een inventarisering, rationalisering en centralisering van de bewaartermijnen. Anderzijds wordt ook gewezen op het belang van het behoud van gegevens verder dan de bewaartermijn, bijvoorbeeld voor historisch onderzoek.

Tot slot, crisissituaties zoals een pandemie of natuurrampen kunnen de vrijwaring van onze fundamentele rechten en vrijheden, zoals het recht op privacy en de bescherming van onze persoonsgegevens, op proef stellen. Er wordt dan ook gepleit voor het creëren van een duidelijk rechtskader voor de verwerking van persoonsgegevens tijdens crisissituaties. Dit moet niet alleen meer rechtszekerheid bieden ten opzichte van de vrijwaring onze fundamentele rechten en vrijheden. De openbare diensten die belast zijn met het beheer van crisissituaties dienen ook op een pragmatische

manier hun wettelijke opdrachten te kunnen uitoefenen. Een duidelijk rechtskader moet de juiste balans strijken tussen de verschillende belangen. Anderzijds wordt ervoor gepleit om de toepasselijke regelgeving niet te rigide te interpreteren en toe te passen. Er wordt gewezen op het evenwicht tussen grondrechten, waarbij het recht op privacy en gegevensbescherming moet afgewogen worden tegen andere fundamentele rechten. Zo wordt de aanpak van de Gegevensbeschermingsautoriteit ten opzichte van dergelijke crisissituaties niet over de ganse lijn positief onthaald.

Duidelijke rechtsgronden voor gegevensverwerkingen. Er is nood aan een duidelijke en gepaste wettelijke basis voor gegevensverwerkingen op lokaal, regionaal of sectoraal niveau. Er wordt vastgesteld dat algemene normen een rechtsgrond voorzien maar zij bieden onvoldoende duidelijkheid over privacybescherming, gegevensstromen en informatieveiligheid (bijv. bij intergemeentelijke samenwerking, publiek-private partnerschappen, gegevensuitwisseling met de lokale politie,...)

Er wordt ook gevraagd naar meer duiding bij de verwerkingen die steunen op het algemeen of vitaal belang. Dit zijn legitieme rechtsgronden maar gebaseerd op concepten die vaak ruimte laten voor een brede of vage interpretatie. Dit maakt het moeilijk de grenzen van deze rechtsgronden af te bakenen hetgeen op zijn beurt kan leiden tot situaties die haaks staan op andere gegevensverwerkingsprincipes zoals de finaliteiten van de verwerking. Een algemene of vage rechtsgrond kan immers leiden tot een (te) brede invulling van de eigenlijke doelstelling van de verwerking. De scheidingslijn tussen de initiële en wat een verdere verwerking van een persoonsgegeven is kan daardoor onder druk staan.

Dit hangt bijvoorbeeld nauw samen met de problematiek van de notie 'overheidsinstantie' wat heel wat implicaties kan hebben niet alleen naar de rechtsgrond voor de verwerking van persoonsgegevens maar ook het regime dat van toepassing is op die verwerkingen (zoals de uitsluiting van administratieve geldboetes). Vanuit de academische wereld wordt ook verzocht dat de wetgever expliciteert dat het algemeen belang een rechtsgrond is waarop universiteiten en hogescholen kunnen terugvallen om wetenschappelijk onderzoek te verrichten.

Betere afstemming met en tussen sectorale wettelijke privacybepalingen. Herhaaldelijk is de vraag teruggekomen naar een duidelijker wettelijk kader inzake gegevensbescherming in sectorale wetgeving (bijvoorbeeld de camerawetgeving, bestuursdecreten, de pandemiewetgeving, ...) en betere duiding over de rechtsgronden waarop men zich kan beroepen. Ook de impact van bepaalde sectorale wetgeving op de verwerking van persoonsgegevens door privéorganisaties en met name de verplichtingen in hoofde van de verwerkingsverantwoordelijken om hun bijstand te verlenen aan veiligheids- of strafrechtelijke doeleinden leidt voor tot bijkomende administratieve lasten en rechtsonzekerheid.

Anderzijds wordt ook gewezen op het bestaan van een waaier aan regelgevingsinstrumenten in bepaalde sectoren die niet op elkaar afgestemd zijn en aldus remmend kunnen werken op de verwerking van persoonsgegevens voor innovatieve toepassingen. Bovendien zou de Privacywet zelf ook beter kunnen afgestemd worden op de noden van bepaalde beroepsgroepen, bijvoorbeeld de verzekeringssector, advocaten of curatoren.

Er is nood aan een grotere juridische coherentie tussen conflicterende regelgeving waardoor verwerkingsverantwoordelijken in de onzekerheid blijven over welke gegevens kunnen verwerkt

worden en welke wettelijk moeten verwerkt worden, bijvoorbeeld in de verzekerings- en financiële sector.

Betere afstemming met andere types van wetgeving. De verhouding tot andere wetgeving is niet altijd duidelijk. Zo is het voor publieke diensten moeilijk om de verplichtingen inzake administratieve openbaarheid of het hergebruik van gegevens in balans te brengen met de verplichtingen inzake gegevensbescherming. Ook voor de advocatuur staat de privacywetgeving soms op gespannen voet met de verplichtingen inzake het beroepsgeheim. Zo zou moeten worden verduidelijkt dat de aanwezigheid van een vertegenwoordiger van de stafhouder vereist is tijdens een controle ter plaatse door een toezichthoudende autoriteit. Hetzelfde geldt in de gezondheidssector waar wordt gepleit voor een verduidelijking in de Privacywet omtrent de verhouding tot het medisch beroepsgeheim. De evolutie vanuit de overheid om via digitale kanalen en platformen steeds meer gezondheidsgegevens te delen vanuit zorgverstrekkers en -instellingen naar derden die een therapeutische relatie met de patiënt moeten aantonen doet bij sommigen vragen rijzen rond de verantwoordelijkheid van de gegevensverstrekende partij. De digitalisering van de samenleving en in het bijzonder de (openbare) dienstverlening plaatst het beroepsgeheim voor nieuwe uitdagingen. De wijze waarop de privacyregels ten opzichte van en door houders van het beroepsgeheim worden ingevuld vereist verdere analyse en debat. Zo wordt bijvoorbeeld de vraag gesteld of we eerder evolueren naar een model van een gezamenlijke gegevensverantwoordelijkheid.

Het aanvullen van de wettelijke verplichtingen van de AVG. Er wordt opgemerkt dat de Belgische wetgever vrij beperkt gebruik heeft gemaakt van de open clausules van de AVG, met andere woorden de bepalingen in de AVG die de lidstaten toelaten om aanvullende regels in te voeren. Volgens sommigen zou België hierin verder kunnen gaan, bijvoorbeeld op het vlak van personeelsmiddelen of de verwerking van gevoelige gegevens (de zogenaamde bijzondere categorieën van persoonsgegevens volgens de AVG). Er wordt op gewezen dat de rechtsgronden voor de verwerking van bepaalde categorieën van bijzondere persoonsgegevens ontoereikend zijn voor bepaalde sectoren. In het bijzonder voor de verwerking van gezondheidsgegevens en gerechtelijke gegevens door private ondernemingen (bijvoorbeeld de verzekeringssector) dringt een uitbreiding van het wettelijk kader zich op. Ook de niet-invulling van de principes van de privacybescherming in een arbeidsrechtelijke context zou leiden tot rechtsonzekerheid. Dit bemoeilijkt het sociaal overleg over privacy. Ook wordt ervoor gepleit om de rol van vakbonden als verwerkingsverantwoordelijke bij het gebruik van kiezerslijsten in het kader van sociale verkiezingen beter te omkaderen. Algemeen heeft België met het aannemen van de Privacywet de kans om een duidelijk kader voor de verwerking van persoonsgegevens in het kader van de arbeidsverhouding laten liggen.

Ook voor de verwerking van biometrische gegevens heeft België nagelaten een specifiek rechtskader te voorzien. Nochtans kan het groeiend belang van deze categorie van gegevens moeilijk nog ontkend worden. Ook op het vlak van arbeidsverhoudingen, het gebruik van cookies, direct marketing en de verwerking van big data en artificiële intelligentie wordt gewezen op de noodzaak van bijkomende regelgeving.

Volgens anderen moet gewaakt worden over de harmonisering van de Europese standaarden. Het toepassen van de open clausules dringt het voordeel van een eengemaakte regelgeving terug en bemoeilijkt de toepassing van de privacywetgeving. Dit is bijvoorbeeld het geval voor de

toestemmingsdrempel van minderjarigen die in België op 13 jaar werd gelegd (cfr. artikel 7 van de Privacywet). Verschillende interpretaties en toepassingen van het reglementaire kader over de EU-lidstaten heen belemmert de werkzaamheden van ondernemingen in hun internationale samenwerking.

3.2. Coherentie in de werking en toepassing van het gegevensbeschermingskader

Een pragmatische aanpak. De toepassing van de privacywetgeving wordt als een zware administratieve last ervaren, in het bijzonder door kleine en middelgrote ondernemingen. Sommige sectoren pleiten er daarom voor dat een hervorming van de Privacywet de administratieve verplichtingen voor ogen moet houden en waar mogelijk moet vermijden om bijkomende lasten op te leggen. In dezelfde lijn wordt gewezen op de noodzaak voor meer flexibiliteit en pragmatisme in de toepassing van privacyregels. In het kader van de verwerking van persoonsgegevens door de academische wereld wordt bijvoorbeeld geopperd om het uitzonderingsregime dat krachtens artikel 24 van de Privacywet van toepassing is op academische publicaties en de uitoefening van de vrije meningsuiting te moet waarborgen verder uit te breiden en los te koppelen van de eigenlijke publicatie van onderzoeksresultaten.

Een factor die bijdraagt tot het bestaan van bijkomende administratieve lasten en rechtsonzekerheid is een gebrek aan een overkoepelende nationale aanpak inzake gegevensbescherming. Zo wordt het voorbeeld geciteerd van het moeten afsluiten van meerdere protocollen of akkoorden om gegevens te kunnen uitwisselen tussen verschillende niveaus of diensten. Het ontbreken van een harmonisering tussen de verschillende beleidsniveaus bemoeilijkt en vertraagt de uitwisseling van gegevens en verzwakt de bescherming van de rechten van de burger. Een concrete maatregel die aan deze bezorgdheid tegemoet zou kunnen komen is het afsluiten van een samenwerkingsakkoord tussen de Federale Staat, de Gemeenschappen en de Gewesten.

De hoedanigheid van verwerkingsverantwoordelijke en verwerker. De AVG en de Privacywet kennen verschillende hoedanigheden toe aan zij die instaan voor de verwerking van persoonsgegevens. Hoofdzakelijk wordt een onderscheid gemaakt tussen de verwerkingsverantwoordelijke en de verwerker. Elke hoedanigheid brengt specifieke verplichtingen met zich mee. De criteria voor de aanduiding van de verwerkingsverantwoordelijke, in het bijzonder in geval van gegevensverwerkingen die complex zijn en waarbij meerdere entiteiten gegevens aanleveren, verwerken of doorgeven, worden echter als onduidelijk ervaren. Dit is in het bijzonder het geval voor de publieke sector. Zo bestaan er geen centrale richtlijnen over de aanduiding in wetgeving van de verwerkingsverantwoordelijke voor gegevensverwerkingen door openbare diensten. In sommige gevallen wordt een minister aangeduid, in andere gevallen het hoofd van een openbare dienst en in nog andere gevallen een departement van een openbare dienst. Algemeen leidt dit niet alleen tot een inconsequente toepassing van de rechtsbeginselen inzake privacy, in het bijzonder het principe van de verantwoording. Het creëert vaak ook een situatie waarin de juridische aanduiding van de verwerkingsverantwoordelijke niet overeenkomt met de feitelijke situatie met betrekking tot de entiteit die de doeleinden en de middelen van de gegevensverwerking bepaalt hetgeen de beslissende factor is om te bepalen wie als verwerkingsverantwoordelijke moet worden aangeduid.

Daarnaast verdient ook de rol van de verwerker en de verhouding tot de verwerkingsverantwoordelijke meer aandacht. Sommige verwerkers kunnen immers omwille van hun dominantie als verwerkingsverantwoordelijken gekwalificeerd worden. Over deze onderlinge krachtmetingen zouden de nationale en Europese toezichthoudende autoriteiten meer duiding en richtlijnen moeten verschaffen.

Divergenties tussen de toezichthoudende autoriteiten. Het bestaan van verschillende gegevensbeschermingsregimes naargelang van het type van autoriteiten en gegevensverwerkingen gaat ook gepaard met opsplitsing van de controlebevoegdheden aan meerdere toezichthoudende autoriteiten. De eerder vermelde onduidelijkheid die soms heerst over de afbakening tussen de gegevensbeschermingsregimes heeft echter ook zijn weerslag op het optreden van deze toezichthoudende autoriteiten. Het gebrek aan een coherent en duidelijk rechtskader maakt met andere woorden dat ook hun adviezen, aanbevelingen en richtlijnen verschillend of afwijkend kunnen zijn ten opzichte van elkaar. Dit plaatst zowel verwerkers van persoonsgegevens als burgers voor soms onduidelijke situaties. Een coherente en correcte toepassing van de wetgeving vereist dan ook dat de risico's op verschillende interpretaties van de privacywetgeving worden geminimaliseerd.

Beschikbaarheid van de toezichthoudende autoriteiten. Ook al worden de toezichthoudende autoriteiten soms afgeschilderd als zij die de stok achter de deur houden en draconische maatregelen opleggen, zij spelen evengoed een rol in het begeleiden van de organisaties die persoonsgegevens verwerken. Dit geldt in het bijzonder voor de Gegevensbeschermingsautoriteit die inderdaad krachtens de AVG over een sterk arsenaal aan corrigerende en sanctionerende maatregelen beschikt. De Belgische wetgever heeft in 2017 met de oprichting van de Gegevensbeschermingsautoriteit echter ook de nadruk gelegd op het belang van een ondersteunende en adviserende rol jegens gegevensverwerkers. Dit veronderstelt een laagdrempelige en vlotte beschikbaarheid van de toezichthoudende autoriteit enerzijds maar ook een proactief begeleidend optreden anderzijds. De mate waarin de toezichthoudende autoriteiten en in het bijzonder de Gegevensbeschermingsautoriteit aan deze verwachtingen kunnen voldoen is afhankelijk van verschillende factoren die nog uitgebreid aan bod zullen komen in dit rapport. De toegankelijkheid en beschikbaarheid van de toezichthoudende autoriteiten om tijdig en altijd geraadpleegd te kunnen worden is echter een basisvereiste voor een coherentie en correcte toepassing van de Privacywet in hoofde van alle betrokkenen.

3.3. Transparantie en vertrouwen in het gebruik van persoonsgegevens

Een wervend verhaal voor de Privacywet. Ook al zijn data alomtegenwoordig in ons dagelijks leven en gaat er geen dag voorbij of er wordt gewezen op de risico's en opportuniteiten van automatiserings- en digitaliseringsprocessen, toch wordt erop gewezen dat het de Privacywet in de eerste plaats misschien ontbreekt aan een verduidelijking van zijn eigen bestaansreden. Persoonsgegevens liggen aan de basis van de digitale transformatie van onze samenleving en dus van ons individueel bestaan en onze interactie als een collectiviteit. De nieuwe technologieën die deze razendsnelle ontwikkelingen voortstuwen worden gevoed met onze persoonsgegevens. Er wordt dan ook gesuggereerd om een debat te houden over het belang van data en gegevensbescherming en de richting waarmee we uit

willen gaan met deze maatschappelijke ontwikkelingen. Een privacywet zou bovenal als principe moeten hanteren dat datagedreven nieuwe technologieën ten dienste moeten staan van de mensheid en in geen geval de mens en een harmonieuze samenleving zouden mogen schaden.

Een beter begrip van de toepasselijke wetgeving.

Gemakkelijk toegankelijke en verstaanbare privacyverklaringen zijn een weerspiegeling van de nood aan transparantie, voorzienbaarheid en duidelijkheid over de wijze waarop persoonsgegevens worden verzameld, verwerkt en doorgegeven. Ook op dit vlak kunnen nog reuzestappen gezet worden. De complexiteit van de technologische evolutie, zij het op wetgevend dan wel op technisch vlak, vereist een vulgarisering van de diensten en instrumenten die ons begeleiden in onze dagelijks private en professionele bezigheden.

Verschillende maatregelen kunnen hiervoor ontwikkeld worden. Zo wordt bijvoorbeeld voorgesteld dat de Privacywet uitdrukkelijk de verplichting zou vermelden voor de overheidsdiensten om een privacyverklaring beschikbaar te stellen van de burger. Vanuit het standpunt dat de overheid als voorbeeld moet gelden zou de Privacywet kunnen voorzien in een minimumkader wat dergelijke privacyverklaringen betreft, mits uitzondering voor bepaalde specifieke diensten die opgesomd zijn in de Titels 2 en 3. Ook een jaarverslag inzake privacybescherming zou deel kunnen uitmaken van dit wettelijk kader. Ruimer dan dat zou de overheid op een eenvoudige manier alle informatie over de privacywetgeving moeten bundelen en beschikbaar maken via een website. Specifiek in de gezondheidssector wordt ervoor gepleit dat alle gezondheidswebsites en – portalen beschikken over een duidelijke, eenvoudige en volledige privacyverklaring. Buiten de overheidssector om zouden alle organisaties die instaan voor de verwerking ook gebaat zijn bij een betere begeleiding omtrent de inhoud van een privacyverklaring.

Ook ruimer dan het beschikbaar stellen van een heldere privacyverklaring moet de overheid meer inzetten op het toepassen van haar eigen transparantieplichting inzake gegevensverwerkingen. De burger weet onvoldoende welke gegevens door welke instantie en voor welke finaliteit worden gebruikt. Ook de link tussen politieke beslissingen en de data die aan de basis liggen van een beslissing is onvoldoende transparant. Er wordt daarom gepleit voor een centraal digitaal platform waarop de burger op een laagdrempelige manier toegang heeft tot deze informatie en in de mate dat dit juridisch mogelijk is de toegang tot en het gebruik van zijn persoonsgegevens kan beheren.

Het uitwerken van een kadaster van persoonsgegevens beheerd door overheidsdiensten wordt aangehaald als een stap in de goede richting. Dit mag zich echter niet beperken tot het catalogeren van gegevensbanken. Evengoed dienen de kruising van gegevens aan de hand van processen of instrumenten zoals datamining, datamatching en datawarehouses opgenomen te worden in dit kadaster. Eenzelfde nood aan transparantie geldt voor de privacyimpactanalyses die door overheidsinstanties worden uitgevoerd en de adviezen van de Gegevensbeschermingsautoriteit over deze analyses. In het bijzonder wat betreft de ontwikkeling en het gebruiken van innovatieve

“Er moet op worden gewezen dat het doel van gegevensbescherming niet erg duidelijk in de kaderwet is opgenomen en dat het goed zou zijn eraan te herinneren dat nieuwe technologieën ten dienste moeten staan van de mensheid en in geen geval schadelijk mogen zijn. Het is dan ook aan de hand van een volledige transparantie ten opzichte van de betrokkenen dat de vertrouwensrelatie kan hersteld worden en zij meer bereid zullen zijn om hun gegevens te delen.” (een deelstatelijke overheid)

toepassingen zou de publicatie van deze analyses en adviezen de burger inzicht geven in de conformiteit met de privacywetgeving.

De essentiële elementen van gegevensbescherming in elke relevante wetgeving. De basisprincipes van de gegevensverwerking, ook wel de essentiële elementen genoemd (finaliteit van de verwerking, categorieën van gegevens, bestemmelingen, ...), zouden in elke wetgeving moeten opgenomen worden waarbij sprake is van gegevensverwerkingen of gegevensstromen. Er wordt vastgesteld dat nog veel bestaande en oude wetgeving nalaat om deze basisprincipes te voorzien. Ook in meer recente wetgeving blijft dit een aandachtspunt en worden de basisprincipes nog te vaak in algemene termen ingevuld. Op die manier wordt te veel ruimte gelaten aan de verwerkingsverantwoordelijken waardoor het gegevensbeheer aan voorzienbaarheid inboet. De mogelijkheid bijvoorbeeld voor overheidsinstanties om persoonsgegevens verder te verwerken of door te geven in “zowel gepseudonimiseerde of geanonimiseerde vorm” biedt geen zicht op hoe de verdere verwerking concreet zal gebeuren.

Zoals eerder vermeld stelt dit probleem zich ook ten opzichte van het bestaan van een duidelijke rechtsgrond voor de verwerking van persoonsgegevens, in het bijzonder door overheidsdiensten. In de uitoefening van hun wettelijke opdrachten initiëren overheidsdiensten soms gegevensverwerkingen waarvoor geen expliciete of aparte rechtsgrond werd bepaald. Er wordt vaak gesteund op een algemene rechtsgrond als een wettelijke opdracht of de uitoefening van een opdracht in het algemeen belang. Transparantie en vertrouwen in een correct beheer van persoonsgegevens door de overheid vereist echter een specifieke wettelijke afbakening in het bijzonder voor complexe of gevoelige gegevensverwerkingen. Daarnaast zou de transparantie verhogen door het creëren van sectorale gegevensbeschermingswetgeving voor openbare diensten.

Tot slot wordt ook gewezen op het belang van de invulling en uitvoering van de verplichting om de nodige en gepaste organisatorische en technische maatregelen te nemen opdat de verwerking van de persoonsgegevens in een beveiligde omgeving zou plaatsvinden. Het betreft zowel menselijke als technische waarborgen inzake toegang tot en gebruik van persoonsgegevens, het regelmatig uitvoeren van veiligheidsaudits, het aanleggen van logboeken, en dergelijke meer.

Het faciliteren van de toepassing van de wetgeving. Transparantie en vertrouwen gaat ook gepaard met de mate waarin een klimaat wordt gecreëerd waarin de verschillende betrokken partijen in de mogelijkheid worden gesteld om hun verplichtingen te vervullen, verzuchtingen kenbaar te maken of hun wettelijke en statutaire opdrachten uit te voeren. De nodige middelen moeten met andere woorden besteed worden aan de omzetting van een wetgevend kader in de praktijk. Er wordt op gewezen dat dit vaak als van ondergeschikt belang wordt beschouwd binnen organisaties of bij beleidsmakers. Er zijn dus bijkomende investeringen nodig (financieel, materieel, opleiding,...).

Naar meer controle voor de burger over het gebruik van persoonsgegevens. Een manier om het vertrouwen in het beheer van persoonsgegevens te verhogen is door de burger meer controle te geven over zijn eigen gegevens. Uit de evaluatie blijkt dat hiervoor een groot draagvlak bestaat. De federale overheid zou de ontwikkeling van persoonlijke datakluisen kunnen stimuleren door dit concept wettelijk te verankeren en privé-partners te ondersteunen in de ontwikkeling ervan. Dergelijke toepassingen

geven gebruikers de controle terug over hun persoonsgegevens en vereenvoudigen de toepassing van de rechten van de betrokken zoals de overdraagbaarheid van data. Ook de overheid zelf zou deze technologie kunnen gebruiken op de eigen werkvloer en zodoende inzetten op enerzijds een versterking van de privacyrechten van de werknemer en anderzijds op een administratieve vereenvoudiging van bepaalde processen.

Anderzijds wordt gewezen op mogelijke belemmeringen in een correcte en adequate dienstverlening indien het recht op toegang tot en de controle over de eigen persoonsgegevens in absolute zin wordt doorgetrokken. In de gezondheidssector bijvoorbeeld kan de digitale beschikbaarheid van gezondheidsgegevens in hoofde van een patiënt ertoe leiden tot hij of zij melding krijgt van medische vaststellingen alvorens dat een begeleidende zorgverstrekker hiervan kennis heeft genomen. Er wordt dan ook gepleit voor een modulaire toepassing van het recht op toegang in het belang van de patiënt, bijvoorbeeld door een termijn in te voeren alvorens de gezondheidsgegevens beschikbaar worden voor de patiënt. Dit moet ook zorgverstrekkers toelaten aanvullende wettelijke verplichtingen uit te voeren (bijvoorbeeld nagaan of de medische documenten geen gegevens van derden bevatten, geen schadelijke informatie voor de patiënt inhouden, of een patiënt niet onder druk van derden staat). In de context van minderjarigen gelden deze overweging des te meer.

Anderen menen dan weer dat niet het persoonsgegeven centraal moet staan in het beleid maar wel het gebruik ervan door private en publieke organisaties. Er zou ook meer transparantie moeten komen rond het gebruik van algoritmes en de finaliteiten van de verwerking van persoonsgegevens. Specifiek in de overheidssector wordt de idee geopperd om een algoritmeregister voor publieke instanties te ontwikkelen.

Er zou ook meer moeten ingezet worden op publiek-private samenwerking in het beheer van data. Volgens sommigen moet dit paal en perk stellen aan de wildgroei van ongereguleerde innovatieve praktijken. Ruimer dan dat wordt ook gepleit voor een reflectie over meer digitale soevereiniteit. Dit debat kan op meerdere niveaus gevoerd worden (regionaal, nationaal, Europees) en moet zich inschrijven in een globale en coherente databeheerstrategie (bijvoorbeeld ontwikkelen van een eigen cloudsysteem).

De beperking van het opleggen van administratieve geldboetes aan overheidsdiensten. Artikel 221 van de Privacywet voorziet dat het systeem van administratieve geldboetes zoals bepaald in artikel 83 AVG niet van toepassing is op de overheid en hun aangestelden of gemachtigden, tenzij het gaat om een publiekrechtelijke rechtspersoon die goederen of diensten aanbiedt op een markt. Ondanks de beslissing van het Grondwettelijk Hof van 14 januari 2021 waarbij deze bepaling niet als ongrondwettelijk werd beschouwd, wordt de uitsluiting van een deel van de publieke sector als discriminerend ervaren door de privésector. De investeringen die door het bedrijfsleven worden gedaan en de mogelijke impact van sancties ingevolge controles door de toezichthoudende autoriteit staan niet in verhouding ten opzichte van de naleving van de AVG door de publieke sector. Dit kan het vertrouwen van de burger schaden in het beheer van persoonsgegevens door de overheid vermits de perceptie van straffeloosheid kan gecreëerd worden. Het uitsluiten van overheidsinstanties van administratieve geldboetes wordt dan ook door gegevensbeschermingsfunctionarissen in de publieke sector zelf aan de kaak gesteld.

Bovendien stelt dit uitzonderingsregime voor de publieke sector privéorganisaties voor het probleem van de hoofdelijke aansprakelijkheid in geval van gezamenlijke verwerkingsverantwoordelijkheid. In

geval van een inbreuk op de privacywetgeving zou de privéorganisaties volledig de administratieve geldboete moeten dragen. Tot slot wordt ook gewezen op de incoherentie met andere wetgeving. Zo voorziet bijvoorbeeld de omzetting van de NIS-Richtlijn betreffende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen niet in een dergelijk uitzonderingsregime voor publieke instanties. Nochtans beslaat het toepassingsgebied van de NIS-Richtlijn ook persoonsgegevens.

Anderen zijn van mening dat deze uitsluiting moet behouden blijven. Indien een wetswijziging zich zou opdringen dan zou op zijn minst meer duidelijkheid moeten komen over de kwalificering van de overheden die uitgesloten worden of kunnen worden. Wordt de bestaande regeling gehanteerd, dan dient op zijn minst het begrip overheid door de wetgever verder verduidelijkt te worden. Er wordt immers gewezen op de restrictieve interpretatie van de huidige wetgeving door de Gegevensbeschermingsautoriteit waardoor sommige instanties (bijvoorbeeld scholen of universiteiten) toch binnen het toepassingsgebied van artikel 83 AVG vallen en dus een administratieve geldboete kunnen opgelegd worden. Er is dus meer rechtszekerheid nodig over de intentie en de draagwijdte van de wetgever betreffende dit uitzonderingsregime.

Een doeltreffend handhavingsbeleid. Het vertrouwen van de burger in de bescherming van zijn persoonsgegevens veronderstelt dat ook een effectief handhavingsbeleid wordt gevoerd in het geval van een schending van de wetgeving. Misbruik van persoonsgegevens dient daadwerkelijk en efficiënt te worden aangepakt. Het belang hiervan moet geplaatst worden in een ruimere context waarbij fenomenen als hacking, piratage, fake news, desinformatie, online laster en pesterij,... uitwassen zijn van de exponentiële groei van het gebruik van internet in ons dagelijks leven en een serie en constructief gebruik van internetdiensten en nieuwe technologische toepassingen ondermijnen. Tegenover dergelijke fenomenen dienen de controleautoriteiten adequaat uitgerust te zijn.

Specifiek stelt zich de vraag naar de doeltreffendheid van het systeem van strafsancities dat door de AVG en Titel 6 van de Privacywet werd ingevoerd. Tot op heden blijken deze strafsancities niet of nauwelijks gehanteerd. Bovendien wordt onderlijnd dat in sommige gevallen strafsancities boven het hoofd van de verwerkingsverantwoordelijke hangen voor internationale gegevensuitwisselingen waarvoor het onduidelijk of quasi onmogelijk zou zijn om aan de privacystandaarden te voldoen. Zo wordt verwezen naar de gevolgen van het arrest Schrems II en het uitblijven van een nieuwe bilateraal akkoord tussen de Europese Unie en de Verenigde Staten. Tot slot wordt onderlijnd dat de nadruk te veel ligt op sancties en te weinig op bemiddeling.

Tegenstrijdige of concurrerende Europese wetgeving. Er werd reeds aangehaald dat de verhouding tussen de privacywetgeving en andere wetgeving niet altijd duidelijk is. Dit geldt evenzeer ten opzichte van andere Europese wetgeving waar er soms tegenstrijdige of concurrerende Europese rechtsinstrumenten bestaan, bijvoorbeeld de verhouding tussen de AVG en de PSD2-Richtlijn of tussen de AVG en de Antiwitwas-Richtlijn. In andere gevallen betreft het een discrepantie tussen nationale en Europese wetgeving.

Zo stelt zich de vraag in welke mate de wet van 11 april 1994 betreffende de openbaarheid van bestuur van toepassing is op de registers van gegevensverwerking die elke verwerkingsverantwoordelijke krachtens de AVG verplicht dient bij te houden. Deze registers worden vaak als interne documenten

beschouwd en kunnen ook bedrijfsgevoelige gegevens bevatten zoals informatie over de technische en organisatorische veiligheidsmaatregelen die een verwerkingsverantwoordelijke toepast of contractuele informatie over de verwerkers. In het verlengde daarvan stelt zich de vraag tot hoever de transparantieplichtingen van een openbare dienst gelden en in welke mate het opportuun is om naar een centralisering van de registers van verwerkingsactiviteiten te evolueren. Een register van verwerkingsactiviteiten dient immers op maat te worden opgesteld en rekening te houden met de functionaliteiten van de gegevensverwerking die plaatsvindt.

3.4. Ondersteuning en begeleiding in de toepassing van de Privacywet

Meer inzetten op communicatie, sensibilisering en responsabilisering. Ondanks de vooruitgang die sinds het bestaan van de AVG is gemaakt in het bewustzijn over en de behandeling van privacyaspecten van gegevensverwerkingen bestaat er nog veel onduidelijkheid over gegevensbescherming, in het bijzonder bij zelfstandigen en KMO's. Er is dus nood aan meer informatie, communicatie en sensibilisering, bijvoorbeeld over gegevensstromen en gegevensopslag maar evengoed over de bescherming van het privéleven in het algemeen of over ethische kwesties gelinkt aan de bescherming van persoonsgegevens en het privéleven. Ook de burger zou gebaat zijn met meer en betere informatie maar evengoed binnen de publieke sector bestaat nog steeds te veel onwetendheid over de privacywetgeving.

Dit is in sommige gevallen te wijten aan een gebrek aan middelen of aan vormingsmogelijkheden maar de onderliggende reden is vaak het ontbreken van een organisatiecultuur die hieraan prioriteit geeft. Dit brengt alle actoren die betrokken zijn in een gegevensstroom in een moeilijke positie. Wanneer de regels onduidelijk zijn, niet of incoherent worden toegepast of er te weinig wordt geïnvesteerd in het sensibiliseren van de organisatie ontstaan er onvermijdelijk gebreken in de keten van verwerkingsverantwoordelijken, verwerkers, gegevensbeschermingsfunctionarissen, dataleveranciers en datagebruikers. Dit kan uitmonden in het ontbreken van een wettelijke basis om persoonsgegevens te verwerken of het bestaan van een onvolledig of onduidelijk wettelijk kader, het opzetten van informatieverwerkingssystemen die niet voldoen aan geactualiseerde standaarden en dus een veiligheidsrisico vormen, de onmogelijkheid om gevolg te geven aan verzoeken van burgers om hun rechten (toegang, verbetering, wissing,...) gepast en tijdig uit te voeren,...

Een bijzondere rol is daarbij weggelegd voor de toezichthoudende autoriteiten waarvan wordt verwacht dat ze meer investeren in hun begeleidings-, informatie- en ondersteuningsrol. De communicatie naar en met de burger, de verwerkingsverantwoordelijke of de gegevensbeschermingsfunctionaris in het doorlopen van diverse procedures of het uitvoeren van vereiste privacymaatregelen vergt bijkomende inspanningen. Rechtstreekse communicatiekanalen met ondernemingen en privacy professionals, eventueel via sectorfederaties zou positief onthaald worden. Dit zou aan verwerkingsverantwoordelijken en verwerkers toelaten om onmiddellijk bij het ontwikkelen van een gegevensverwerkingsproces rekening te kunnen houden met eventuele bedenkingen van een toezichthoudende autoriteit, eventuele risico's beter te kunnen evalueren en mogelijke sancties in een later stadium te vermijden. Een beter begrip van de noden van een specifieke sector zorgt voor een betere afstemming van de strategische doelstellingen van een toezichthoudende autoriteit.

Het ontwikkelen van ondersteuningsinstrumenten. Er werd reeds op gewezen dat het toepassen van de wettelijke verplichtingen vaak een administratieve last inhoudt die als bureaucratisch, stringent en weinig efficiënt wordt ervaren. Anderzijds werken de vaak nog onduidelijke regels innovatieve processen tegen. Er wordt dan ook breed pleidooi gehouden om een versnelling hoger te schakelen wanneer het erop aankomt om de begeleidings- en ondersteuningsinstrumenten van de AVG te kunnen hanteren. Concrete standaarden, goede praktijken, sectorgeoriënteerde instrumenten en sjablonen - gevalideerd door de toezichthoudende autoriteiten – kunnen het nodige kader bieden om in volle

overeenstemming met de geldende privacystandaarden op een vlottere en meer efficiënte wijze gegevens te verwerken. De toezichthoudende autoriteiten zouden ook hun aanbevelingen en adviezen kunnen harmoniseren en vereenvoudigen, FAQ's en templates ontwikkelen en een eerstelijnsbijstand uitbouwen met een specifieke sectie die zich zou richten op de ondersteuning en controle van overheidsdiensten.

De voorzienbaarheid van de toepassing van de beginselen van de AVG en de Privacywet zou ook kunnen verbeterd worden, bijvoorbeeld aan de hand van een mechanisme van 'privacy

« De AVG voorziet in een instrumentarium dat voor alle soorten ondernemingen en organisaties beschikbaar is als hulpmiddel om te laten zien hoe de wetgeving kan worden nageleefd, zoals gedragscodes, certificeringsmechanismen en modelcontractbepalingen. Dit instrumentarium moet ten volle worden benut. Kleine en middelgrote ondernemingen wijzen er in het bijzonder op hoe belangrijk en nuttig het is dat gedragscodes op hun situatie zijn afgestemd en geen buitensporige kosten of lasten met zich mogen meebrengen. » (Een beroepsfederatie)

rulings'. Dit mechanisme zou de toezichthoudende autoriteit toelaten om de toepassing van de wetgeving te interpreteren naar gelang het individueel geval van gegevensverwerking dat zich aanbiedt. Dit zou de rechtszekerheid, de voorzienbaarheid, de duidelijkheid en de naleving van de wetgeving ten goede komen.

De toepassing van sectorale en thematische gedragscodes zou verwerkingsverantwoordelijken ondersteunen in het bekomen van een privacyconform label. Het kan dan ook een belangrijk instrument zijn voor sectorfederaties maar de ontwikkeling van deze gedragscodes vereist expertise en middelen. Ook hier zouden verwerkingsverantwoordelijken en verwerkers moeten kunnen genieten van een vereenvoudiging van de toepassing van gedragscodes. Een uitbreiding van de gedragscodes kan ook een werklastvermindering voor de toezichthoudende autoriteiten meebrengen.

De ontwikkeling van gedragscodes veronderstelt dat er toezichtmechanismen worden opgericht die de naleving van de gedragscode controleren. Deze mechanismen moeten geaccrediteerd worden door de toezichthoudende autoriteiten. De kosten van de controles en het toezicht op de naleving van de gedragscodes moeten echter in verhouding staan tot de capaciteiten van sectorfederaties. Voor sommige beroepsfederaties is het ook niet haalbaar om een onafhankelijk toezichtsorgaan te voorzien. Bovendien moeten de gedragscodes op maat geschreven worden. Indien de lat te hoog zou worden gelegd is het mogelijk dat sommige sectoren bepaalde standaarden niet kunnen halen hetgeen zou leiden tot een concurrentieel nadeel door uitsluiting van markttoegang.

Ook certificeringssystemen kunnen verwerkingsverantwoordelijken ondersteunen, de toepassing van de privacyregels begeleiden en de bescherming van persoonsgegevens versterken, bijvoorbeeld voor de verwerking van gevoelige gegevens. Zo kan certificering gebruikt worden door

verwerkingsverantwoordelijken om aan te tonen dat ze van bij de conceptualisering van gegevensverwerkingsprocessen en als standaard privacybeschermende maatregelen treffen. BELAC als nationale certificeringsautoriteit kan hierin een centrale rol spelen.

De toepassing van privacyimpactanalyses. Verwerkingsverantwoordelijken en verwerkers hebben ook behoefte aan een betere begeleiding in het inschatten van en omgaan met risico's. Impactanalyses vormen een belangrijk instrument daarbij maar worden nog te weinig consequent gebruikt. Een deel van de verklaring ligt bij het ontbreken van richtlijnen over de voorwaarden en de modaliteiten van de toepassing van een privacyimpactanalyse. Dit is bijvoorbeeld het geval tijdens het wetgevend proces. Verwerkingsverantwoordelijken hebben duiding nodig over basisvragen zoals het tijdstip waarop een analyse moet uitgevoerd worden, vanaf welk moment dit kan of moet in de totstandkoming van een gegevensverwerkingsproces en of een impactanalyse gerationaliseerd en gecentraliseerd kan worden in geval er meerdere partijen betrokken zijn.

Bovendien dient ook een meer globale methodologie te worden aangenomen rond het gebruik van gegevensbeschermingsimpactanalyses. Een verwerkingsverantwoordelijke dient niet enkel een risico in te schatten aan de hand van het noodzakelijkheids- en proportionaliteitsprincipe. Het intrusieve karakter van een gegevensverwerking dient in een bredere context te worden geanalyseerd. Vanuit het terrein klinkt dan ook de nood aan meer begeleiding om dergelijke vaak complexe oefeningen te kunnen uitvoeren, en waar mogelijk in samenwerking met de toezichthoudende autoriteiten.

Sectorgebonden expertise binnen de toezichthoudende autoriteiten. Herhaaldelijk wordt gewezen op de nood tot het aanduiden van aanspreekpunten binnen de Gegevensbeschermingsautoriteit voor een bepaalde sector en/of expertise. Vanuit het terrein klinkt vaak de roep naar toezichthoudende autoriteiten die voeling hebben met de noden en de specificiteit van sectorgebonden verwerkingen. Een geïnformeerde, correcte en haalbare toepassing van de privacywetgeving vereist een kruisbestuiving tussen verschillende expertisedomeinen, privacy en technologie. Zowel de politiek, het juridische als het technische spelen ook een belangrijke rol in het ontwikkelen en toepassen van wetgevende normen. Het opbouwen van een dialoog, een debat in tweerichtingsverkeer waarbij feedback wordt gegeven, maakt dat toezichthoudende autoriteiten een hands-on adviesverlening kunnen bieden. In het bijzonder in het geval van datalekken bijvoorbeeld is het cruciaal dat kort op de bal wordt gespeeld.

Er wordt ook gesuggereerd dat er binnen de Gegevensbeschermingsautoriteit een helpdesk zou kunnen worden opgericht om gratis en onverwijld informatie te kunnen verkrijgen over de toepassing van de Privacywet en aanverwante sectorale of Europese regelgeving.

In dezelfde lijn en specifiek wat betreft de Gegevensbeschermingsautoriteit wordt ook gewezen op het uitblijven van de oprichting van de reflectieraad. De reflectieraad is een orgaan onafhankelijk van de Gegevensbeschermingsautoriteit die niet-bindende adviezen kan verlenen, bijvoorbeeld over het strategisch plan waarin de prioriteiten van het directiecomité worden uitgestippeld. De ratio legis van deze reflectieraad is dat aan de hand van een multidisciplinaire samenstelling zij ervoor zorgt dat de Gegevensbeschermingsautoriteit voeling blijft hebben met wat leeft op het terrein en in de praktijk. Een dergelijk orgaan wordt algemeen als wenselijk en nuttig beschouwd maar werd dus tot op heden door de Kamer van volksvertegenwoordigers nog niet opgericht.

3.5. Een kader voor innovatie

Nood aan een globaal databeheerbeleid. De Belgische privacywetgeving vloeit voort uit een Europees kader waarvan de bescherming van persoonsgegevens de hoeksteen vormt. Een informatiesysteem of gegevensverwerkingsproces is vaak echter complexer dan louter een verwerking van persoonsgegevens en bestaat ook uit niet-persoonsgegevens. Digitalisering en innovatie steunen immers niet enkel op persoonsgegevens maar data in de brede zin van het woord. Bovendien is de bescherming gericht op natuurlijke personen en kan de vraag gesteld worden in welke mate ook rechtspersonen moeten kunnen genieten van een bepaald beschermingsniveau. Algemeen is er dus nood aan een beleid waarbij niet alleen rekening wordt gehouden met de privacybeschermende dimensie van gegevensverwerkingen maar tevens een globale visie wordt uitgestippeld inzake gegevensbeheer.

Het huidige versnipperde en onvolledige wettelijke landschap inzake gegevensbeheer heeft een remmend effect op innovatieve ontwikkelingen. Het faciliteren van gegevensuitwisselingen van welke aard ook en het stimuleren van innovatie aan de hand van nieuwe technologieën vereist een passend beleids- en wetgevend kader. Dergelijk objectief moet België ook in staat stellen om versnelling hoger te schakelen in de ontwikkeling van een kenniseconomie zodat we ons sterker kunnen positioneren tegenover digitale platformen die een quasi monopolie positie hebben ingenomen op de markt. De controle over het beheer van data staat centraal in het maximaliseren van de uitwisseling van gegevens. Evengoed zou België met dergelijk objectief kunnen beantwoorden aan bepaalde internationale verplichtingen. Zo wordt België vaak door internationale organen met de vinger gewezen over het tekort aan statistische gegevens. Ook hier moet België een tandje bijsteken. Bovendien zijn er ook andere dimensies die aan bod moeten komen, breder dan het juridische en informatieveiligheidsperspectief, bijvoorbeeld ethische kwesties. Ook in dat opzicht schiet de Belgische wetgeving tekort.

Bovendien moeten we ook rekening houden met de impact van digitalisering op het milieu. De grondstoffen die mee aan de basis liggen van de ontwikkeling van nieuwe technologieën zijn niet oneindig beschikbaar. Er wordt dan ook voorgesteld na te denken over een beleid waarin het delen van digitale diensten mogelijk is zodat de consumptie ervan vermindert. Standaardisering, interoperabiliteit en hergebruik van gegevens kunnen daarin een leidraad vormen.

Meer algemeen zou de overheid nog meer dienen te steunen op het gebruik van data in het beleidsvormings- en -beslissingsproces. Tegelijk wordt ook gepleit voor een debat over de grenzen van innovatie en nieuwe technologieën. De AVG biedt een kader, bijvoorbeeld inzake het gebruik van persoonsgegevens voor profilering, maar dit kader moet nationaal of Europees verder ingevuld worden. De AVG is ook een technologie-neutraal reguleringsinstrument dat verder aangevuld wordt door sectorspecifieke (bijvoorbeeld inzake elektronische communicatie met de e-Privacyrichtlijn) of thematische wetgeving (bijvoorbeeld het ontwerp van verordening inzake artificiële intelligentie).

De Privacywet is met andere woorden een schakel in een groter geheel. Een wet betreffende een transparant en efficiënt databeheer kan een sluitend antwoord bieden op al deze dimensies en uitdagingen.

Een meer open invulling van het toezichthoudende mandaat. Ook de toezichthoudende autoriteiten zouden een meer gediversifieerde aanpak kunnen hanteren eerder dan zich louter te positioneren als

de waakhond van de gegevensbescherming van de burger. Er wordt opgemerkt dat het mandaat dat hen krachtens de AVG is gegeven ruimer is en dat zij evengoed rekening moeten houden met het belang van innovatie en digitalisering. In het bijzonder moeten de toezichthoudende autoriteiten in staat zijn om al in een vroeg stadium de ontwerpprocessen van nieuwe technologieën te begeleiden, bijvoorbeeld in het geval van verwerking van biometrische gegevens of toepassing van artificiële intelligentie.

De toezichthoudende autoriteiten zouden ook een duidelijker standpunt kunnen innemen in privacykwesties. Daarvoor is het uiteraard belangrijk dat hun onafhankelijkheid gerespecteerd wordt. Enkel zo kan een toezichthoudende autoriteit ten volle aan maatschappelijke debatten deelnemen of initiëren.

Inzetten op de eigen Europese kracht. De Amerikaanse dominantie op het vlak van internettechnologie en daarmee verbonden diensten zou moeten doorbroken worden. De Europese visie op privacy en gegevensbescherming kan gerealiseerd worden door meer gebruik te maken van Europese internettechnologie. Voor zover overheidsdiensten zich dienen te beroepen op dienstverlening van GAFA-type ondernemingen zou er kunnen worden voorzien in een strategisch vendor management naar analogie met Nederland. Het sluiten van contracten op het niveau van individuele overheidsdiensten plaatst ons in een zwakkere onderhandelingspositie. Het optillen van de onderhandelingen naar een centraal en gecoördineerd niveau zou de Belgische overheden moeten toelaten om meer gunstige voorwaarden af te dwingen. Dit heeft ook zijn belang ten aanzien van de contractuele clausules als verwerker van persoonsgegevens van Belgische burgers en residenten.

Het principe van dataminimalisering moet centraal staan in elk innovatief initiatief inzake gegevensverwerking. In de overheidssector zou de problematiek van de verwerking van persoonsgegevens en het gebruik van algoritmes centraal moeten staan in het kader van overheidsopdrachten. Standaardclausules over het gebruik van data zouden rechtszekerheid bieden en een level-playing field waardoor de drempel zou verlagen voor kleinere digitale spelers om in te schrijven op overheidsopdrachten, in het bijzonder voor innovatieve projecten.

Het concept van de ‘regulatory sandboxes’ komt herhaaldelijk terug als aandachtspunt. Het voorzien van een uitdrukkelijk wettelijk kader hiervoor beantwoordt aan de nood aan flexibiliteit bij de toepassing van bestaande regelgeving of moet het ontbreken van sectorspecifieke regelgeving compenseren. Dit mechanisme maakt het mogelijk om onder bepaalde voorwaarden en in samenspraak met de betrokken toezichthoudende autoriteiten proefprojecten op te zetten. Met andere woorden, er wordt een kader opgezet waarin de regelgevingsdrempel wordt verlaagd om innovatie te stimuleren en te ondersteunen. Bedrijven krijgen aldus de kans om live te testen en marktacceptatie te verkrijgen.

De plaats van de toestemming als rechtsgrond voor gegevensverwerkingen. Toestemming als rechtsgrond botst vaak met voortschrijdende technologische ontwikkelingen. Een te stringent gegevensbeschermend kader kan ook een tegenovergesteld effect en een negatieve connotatie veroorzaken bij de gebruiker van nieuwe technologieën. Er zou dus een debat moet gevoerd worden over het belang van de toestemming als rechtsgrond voor de verwerking van persoonsgegevens.

Er zijn ook sectoren waarin de toestemming als rechtsgrond de verwerking van persoonsgegevens bemoeilijkt, bijvoorbeeld voor verzekeraars of wetenschappelijk onderzoekers. Een persoon beschikt over het recht om te allen tijde zijn toestemming in te trekken hetgeen het beëindigen van bepaalde

verwerkingen vóór het afsluiten van een contract in het gedrang brengt. Ook wetenschappelijk onderzoek kan gehinderd worden door te moeten terugvallen op toestemming als rechtsgrond. Er wordt daarom gepleit om in het kader van artikel 9, § 4 AVG gebruik te maken van de mogelijkheid om, bijvoorbeeld voor gezondheidsgegevens, een aanvullend wettelijk kader te voorzien waarbij het afsluiten van een contract als rechtsgrond wordt beschouwd eerder dan de toestemming.

Er kan echter geen eenduidige lijn worden getrokken in het debat over de invulling van de toestemming als rechtsgrond. In de gezondheidssector wordt enerzijds gepleit voor de nodige flexibiliteit en de expliciete vermelding in de Privacywet opdat zorgverstrekkers het digitale dossier mogen beheren zonder de expliciete voorafgaandelijke toestemming van de patiënt. Ook het gezamenlijk kunnen beheren van een digitaal patiëntendossier tussen ziekenhuisnetwerken door middel van een gemeenschappelijke databank wordt aangestipt als een noodzakelijke ontwikkeling. Anderzijds wordt ook gepleit voor een meer granulaire invulling van de toestemmingsvereiste, bijvoorbeeld om de patiënt meer inspraak te geven over de doorgifte van zijn of haar persoonsgegevens. Ook de verhouding tussen de toestemming van de patiënt als rechtsgrond en de wettelijke verplichting om via digitale kanalen en platformen gezondheidsgegevens te delen plaatst zorgverstrekkers en -instellingen soms voor ethische, juridische en operationele dilemma's.

Op punt stellen van het wettelijk kader voor gegevensverwerkingen in het kader van wetenschappelijk onderzoek. België heeft artikel 89, §§ 2 en 3 AVG in wetgeving omgezet aan de hand van Titel 4 van de Privacywet. De meningen zijn verdeeld over het bestaan van een aparte titel in de Privacywet die van toepassing is op de verwerking van gegevens met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Enerzijds wordt gewezen op de flexibiliteit die de AVG net voor gegevensverwerkingen van dergelijke aard heeft willen invoeren. Het opleggen van bijkomende regelgeving wordt beschouwd als het toevoegen van een complexe laag aan verplichtingen bovenop al bestaande verplichtingen. Zo wordt gewezen op het moeten toevoegen van de privacyimpactanalyses (artikel 191 van de Privacywet) en verwerkingsovereenkomsten (artikel 196 van de Privacywet) aan het gegevensverwerkingsregister of de verplichting om bij de verwerking van gevoelige persoonsgegevens een privacyimpactanalyse te moeten uitvoeren. Bijkomende of afwijkende regelgeving ten opzichte van het Europese kader kan ook als hinderend ervaren worden voor het opzetten van onderzoeksprojecten in Europees verband. Anderzijds wordt wel de noodzaak aangestipt tot verduidelijking – en eventueel een bijkomend regelgevend kader – met betrekking tot de betrokkenheid van studenten in academisch onderzoek en het feit dat een anonimisering of het wissen van persoonsgegevens op private logiciels niet altijd mogelijk is.

Anderen zijn dan weer de invoering van Titel 4 van de Privacywet beter gezind maar wijzen op de moeilijkheden die ze in de praktijk ondervinden in de concrete toepassing ervan. Dit is bijvoorbeeld omwille van onduidelijkheid inzake terminologie, het ontbreken van duiding over de procedurele vereisten, de werkbaarheid van bepaalde verplichtingen en de overlapping met of verhouding tot andere toepasselijke wetgeving (bijvoorbeeld inzake klinische proeven). Ook het mechanisme volgens hetwelk moet gewerkt worden met derde vertrouwenspartijen stelt universiteiten en hogescholen voor bijzondere uitdagingen vermits er op de markt weinig spelers te vinden zijn die aan de voorwaarden van de Privacywet voldoen. Dit heeft voor gevolg dat de investeringskost stijgt. Als alternatief zou kunnen nagedacht worden over het toebedelen van de rol van derde vertrouwenspartijen aan onderzoeksexperten of afdelingen binnen een universiteit zelf.

Gelet op deze hindernissen gebeurt het dan ook dat bepaalde federaties hun leden aanraden om geen gebruik te maken van het uitzonderingsregime van Titel 4 omdat het ook meer verplichtingen inzake compliance vereist dan de loutere toepassing van de AVG. Daarnaast wordt ook gewezen op het beperkte toepassingsgebied van Titel 4. Enkel wanneer de uitoefening van de rechten van de betrokkenen het onderzoek onmogelijk dreigt te maken of kan belemmeren en dus afwijkingen noodzakelijk zijn om de verwerkingsdoelstellingen te bereiken geldt het uitzonderingsregime. Zijn er geen beperkingen vereist, dan is Titel 4 niet van toepassing. In de praktijk leidt dit tot onduidelijkheid. Ook de mogelijkheid om een deel van Titel 4 niet te moeten toepassen voor zover er een gedragscode wordt opgesteld (cfr. artikel 187 van de Privacywet) wordt in de huidige stand van zaken als onwerkbaar beschouwd vermits er geen duidelijkheid is over het orgaan dat zou moeten instaan voor de controle op de toepassing van de gedragscode.

Specifiek in de gezondheidssector wordt gepleit voor het houden van een interfederaal debat over het opzetten van een kader betreffende het ter beschikking stellen van geanonimiseerde of gepseudonimiseerde gezondheidsgegevens voor therapeutische en statistische doelstellingen. Dergelijk debat veronderstelt dat antwoorden worden geboden op diverse problematieken : ethische kwesties, het juridisch vergrendelen van het mogelijk gebruik van dergelijke gegevens, het bepalen van standaarden waaraan vertrouwenspartijen dienen te voldoen, het creëren van een kader voor het ontwikkelen van ‘use cases’,...

Gelet op het belang van gegevensuitwisseling en wetenschappelijk onderzoek voor innovatie dient Titel 4 op punt gesteld te worden. Een vereenvoudiging en versoepeling van het uitzonderingsregime moet België een concurrentieel voordeel bieden ten opzichte van het algemene AVG-kader en moet de beperkingen die verbonden zijn aan wetenschappelijk onderzoek zo veel als mogelijk mitigeren. Dit is in het bijzonder het geval voor wetenschappelijk onderzoek in de gezondheidssector. Ook dient er beter te worden gecommuniceerd over de toepassing van Titel 4 en de concrete implicaties ervan.

3.6. Verbeteren van de gegevensuitwisseling

Vereenvoudiging van het systeem van administratieve protocollen en toegang tot overheidsgegevens.

De verplichting overeenkomstig artikel 20 van de Privacywet voor overheidsdiensten om voor gegevensuitwisselingen protocollen af te sluiten beantwoordt onvoldoende aan de verwachting van de wetgever. Het systeem werd ingevoerd als antwoord op de afschaffing van het vorige systeem van de sectorale comités bij de voormalige Privacycommissie. Teneinde de vrees op te vangen dat het wegvallen van het vangnet van de sectorale comités een remmend effect zou hebben op de uitwisseling van gegevens tussen en vanuit overheidsdiensten werd de mogelijkheid tot het afsluiten van protocollen wettelijk ingevoerd. Dit systeem sluit immers aan bij de letter en de geest van de AVG, met name de verantwoordingsverplichting die maakt dat verwerkingsverantwoordelijken zelf instaan voor het organiseren van de gegevensuitwisselingen en het bepalen van de modaliteiten volgens dewelke dit gebeurt. Parallel hiermee werd ook het Informatieveiligheidscomité opgericht dat aan de hand van beraadslagingen kan tussenkomen bij het bepalen van de modaliteiten van gegevensuitwisselingen.

Dit geheel wordt als te complex, ondoorzichtig en omslachtig beschouwd. De verplichting om individuele protocollen of akkoorden om gegevens te kunnen uitwisselen is een zware administratieve last en dient vereenvoudigd te worden (bijvoorbeeld aan de hand van een vereenvoudigd standaardformulier of het centraal publiceren van de protocollen eerder dan op de websites van elke

individuele verwerkingsverantwoordelijke). Er wordt ook gepleit voor de mogelijkheid om meer algemene protocollen af te kunnen sluiten, bijvoorbeeld in het geval waarbij meerdere partijen betrokken zijn bij gegevensuitwisselingen. Er wordt ook voorgesteld te bestuderen in welke mate het faciliteren van de toegang tot overheidsgegevens zou verbeterd en versneld kunnen worden via de tussenkomst van een mechanisme dat als onafhankelijke derde partij zou kunnen optreden. Ook wordt ervoor gepleit dat de toegang tot gegevens waarover overheden beschikken en in het bijzonder de toegang tot authentieke bronnen gratis zou blijven.

“Deze kaderwet vertegenwoordigt een belangrijke vooruitgang in de zin dat zij echt het accent legt op een grotere transparantie maar evenzeer op een betere controle van de gegevens. Daarenboven verplicht zij publieke instanties een inventaris op te maken van hun verwerkingen en toe te zien op de rechtsgrond en hun wettelijkheid. In veel gevallen heeft dit toegelaten aan hen die een zeker niveau van conformiteit wensten te bereiken om hun verwerkingen in vraag te stellen maar ook hun manier van werken en zodoende hun procedures voor de toegang, extractie en doorgifte van gegevens te wijzigen. Dit zou het verwachte resultaat moeten zijn geweest voor de meerderheid van de publieke instanties maar zwaktes hebben de kaderwet gehinderd in het bereiken van haar doelstellingen.” (Een deelstatelijke overheid)

Aansluitend hierop wordt meer algemeen gewezen op de complexe en logge toegang tot (federale) overheidsgegevens. Naargelang het soort van overheidsgegeven dient een verschillende procedure gevolgd te worden : een beslissing van de minister van Binnenlandse Zaken voor de toegang tot het Rijksregister, een beraadslaging van het Informatieveiligheidscomité voor sociale en gezondheidsgegevens, een protocol conform artikel 20 van de Privacywet of een beraadslaging van het Informatieveiligheidscomité

voor andere federale overheidsgegevens. Bovendien is er nog een lappendeken aan wetgeving die bijzondere regels oplegt via koninklijk besluit voor de toegang tot bepaalde databanken. De toegang tot overheidsgegevens dient daarom op een meer eenvormige en vereenvoudigde manier georganiseerd te worden, eventueel door alle aanvragen voor toegang te laten beoordelen door een onafhankelijke instantie.

Anderzijds dient ook sterker ingezet te worden op het beschikbaar maken van overheidsdata en op het maximaliseren van het gebruik van de beschikbare data. De kwaliteit van de data is daarbij een bijzonder aandachtspunt.

Herzien van de rol van het Informatieveiligheidscomité. Er bestaat een algemene bezorgdheid omtrent het respecteren van de verplichting om te voorzien in een duidelijke en transparante rechtsgrond voor de verwerking van persoonsgegevens. Tegen deze achtergrond wordt de rol en de werking van het Informatieveiligheidscomité in vraag gesteld. De mogelijke invloed van het Informatieveiligheidscomité in het bepalen of het verder uitwerken van de essentiële elementen van een gegevensverwerking kan op gespannen voet staan met de verplichting om deze elementen door de wetgever te laten vastleggen. Bovendien bestaat er onduidelijkheid over de juridische aard van de beslissingen van het Informatieveiligheidscomité en de mogelijkheid om hiertegen beroep in te stellen.

De scheidingslijn met de bevoegdheden van de toezichthoudende autoriteiten, in het bijzonder de Gegevensbeschermingsautoriteit, moet ook verduidelijkt worden. De mate waarin het Informatieveiligheidscomité bepalingen van de AVG zou kunnen interpreteren aan de hand van

beraadslagingen of aanbevelingen doet de vraag rijzen of het Informatieveiligheidscomité zich hiermee niet op het terrein van een onafhankelijk toezichthoudende autoriteit begeeft.

Ook de verhouding tot de verwerkingsverantwoordelijken, in het bijzonder de overheidsadministraties, wordt als problematisch ervaren. Zo kan het Informatieveiligheidscomité optreden op vraag van een enkele overheidsadministratie en aldus bindende aanbevelingen uitvaardigen zonder betrokkenheid van alle overheidsadministraties. Ook wordt aangehaald dat het optreden van het Informatieveiligheidscomité de autonomie van een administratie als verwerkingsverantwoordelijke kan aantasten.

Anderzijds wordt dan weer gewezen op de efficiënte werking van het Informatieveiligheidscomité in vergelijking met andere bestaande toegangsmodaliteiten en wordt gepleit voor het behoud van een dergelijk orgaan.

De invulling van de hoedanigheid van verwerkingsverantwoordelijke. Binnen eenzelfde entiteit (universiteit, overheidsdienst,...) bestaat de mogelijkheid dat op verschillende niveaus verwerkingsverantwoordelijken werden aangeduid. Deze problematiek werd eerder al aangehaald. Het bestaan van meerdere verwerkingsverantwoordelijken binnen eenzelfde entiteit doet echter ook praktische vragen rijzen naar de toepassing van de verschillende verplichtingen krachtens de AVG en de Privacywet. Kan bijvoorbeeld een enkel register van verwerkingsactiviteiten bijgehouden worden of dienen er meerdere te worden opgesteld, een voor iedere individuele verwerkingsverantwoordelijke? Moeten er afspraken gemaakt worden tussen de individuele verwerkingsverantwoordelijken in de vorm van protocollen conform artikel 20 van de Privacywet, verwerkingsovereenkomsten of een akkoord tussen gezamenlijke verwerkingsverantwoordelijken? De verduidelijking van dergelijke vraagstukken heeft een onmiddellijke en praktische impact op het faciliteren van gegevensuitwisselingen.

Een versterking van de werking van de dienstenintegratoren. Het systeem van de dienstenintegratoren wordt als een belangrijke factor in het succes van het beheer van overheidsgegevens beschouwd. De rol van de dienstenintegratoren moet versterkt worden en dit op alle niveaus. Het behalen van de doelstellingen inzake eGovernment, administratieve vereenvoudiging en hergebruik van gegevens zijn hier immers van afhankelijk. De toegang tot authentieke bronnen moet dan ook verder worden uitgebreid. Er dienen ook duidelijker afspraken te worden gemaakt over de rol van de dienstenintegratoren bij de totstandkoming van gegevensuitwisselingen in de publieke sector. De dienstenintegratoren worden immers nog steeds niet altijd hierbij betrokken.

Het gebruik van de dienstenintegratoren voor de uitwisseling van gegevens moet verder gestimuleerd worden. Hun rol zou ook verder kunnen uitgebreid worden, niet alleen beperkt tot de uitwisseling van persoonsgegevens tussen overheidsdiensten maar evengoed ten aanzien van burgers. Bovendien zou de volwaardige uitbouw van de dienstenintegratoren ook de transparantie in de verwerking van persoonsgegevens door de overheid ten goede komen vermits de dienstenintegratie automatisch gegevensstromen repertorieert.

Het uitbreiden van de toegang tot de gegevens van het Rijksregister. Het gebruik van bepaalde persoonsgegevens zoals het rijksregisternummer of de gegevens in het bevolkingsregister die

gereguleerd wordt door bijzondere of sectorale wetgeving zou kunnen bijdragen tot processen van administratieve vereenvoudiging. Het correct identificeren van een persoon speelt een cruciale rol in tal van administratieve processen en wordt ook opgelegd door verschillende regelgevingen. Het uitbreiden van de toegang tot het Rijksregister en het gebruik van het rijksregisternummer zou dan ook aanzienlijk kunnen bijdragen tot de digitale transformatie en de vereenvoudiging van administratieve procedures.

Ook het ontwikkelen van een digitale identificatieportefeuille wordt naar voren geschoven als een instrument om de interactie tussen burgers en privé- of publieke organisaties eenvoudiger te organiseren.

Nood aan een pragmatische interpretatie en toepassing van de Privacywet. De strikte interpretatie van artikel 22 van de Grondwet door de Gegevensbeschermingsautoriteit wordt als een belemmering ervaren op de organisatie door overheidsinstanties van hun gegevensbeheer. De rechtspraak van de Gegevensbeschermingsautoriteit als zou de verwerking van persoonsgegevens in zijn geheel wettelijk of decretaal moeten vastgelegd worden werkt remmend op innovatie, is weinig pragmatisch en houdt geen rekening met de mogelijkheid voor de uitvoerende macht om in het kader van opdrachten van algemeen belang gegevensverwerkingen te kunnen of moeten organiseren.

Ook de aanpak van de Gegevensbeschermingsautoriteit in crisissituaties zoals de corona-pandemie wordt bekritiseerd als te log en te streng. Bovendien zou zij niet in staat zijn om voldoende kort op de bal te spelen waardoor ondernemingen reeds maatregelen hebben ontwikkeld of oplossingen brengen op de markt die nadien niet blijken te stroken met de visie van de Gegevensbeschermingsautoriteit. Dit maakt het moeilijk om in een economisch en sanitair uiterst uitdagende context tot werkbare oplossingen te komen.

3.7. De bescherming van de betrokkenen

Versterking van de toegang tot en de uitoefening van de rechten van betrokkenen. De AVG en de Privacywet bieden een robuust kader van rechten waarop de burger beroep kan doen, niet enkel om misbruik van zijn persoonsgegevens aan te klagen maar evengoed om het beheer van en de controle over zijn persoonsgegevens in handen te nemen. De burger zou dan ook beter wegwijs moeten gemaakt worden in deze waaier van mogelijkheden. Er moet dus meer ingezet worden op het informeren van burgers over hun rechten en in het bijzonder over de mogelijkheid om klacht in te dienen, bijvoorbeeld in het geval van datalekken. Ook in de uitoefening van het recht op toegang tot persoonsgegevens die beheerd worden door overheidsdiensten schiet men nog vaak te kort.

De voorwaarden waaronder de uitoefening van het recht op wissing en verbetering van persoonsgegevens kan of mag plaatsvinden dienen te worden verduidelijkt. Het is voor verwerkingsverantwoordelijken immers niet altijd duidelijk in welke mate de uitoefening van de rechten van betrokkenen kan worden geweigerd.

Er wordt gesuggereerd om een lijst op te stellen en te publiceren van de uitzonderingen die gelden op de rechten van betrokkenen. Ook zou moeten verduidelijkt worden welke de termijnen zijn binnen dewelke een burger recht heeft op een antwoord of een verzoek tot uitoefening van zijn rechten. Vanuit

de vakbondsorganisaties wordt ook gevraagd dat zij kunnen gemachtigd worden om namens een van hun leden een klacht in te dienen en namens hen administratieve of gerechtelijke beroepsmogelijkheden uit te oefenen.

De gespannen verhouding tussen het privacyrecht en het strafrecht. De uitoefening van de rechten van de betrokkenen in het justitiële landschap dient te worden verduidelijkt. Het huidige systeem waarbij de Privacywet verwijst naar het gerechtelijk wetboek, het wetboek van straffordering en bijzondere strafwetgeving biedt onvoldoende duidelijkheid over het bestaan en de toepasbaarheid van de individuele rechten van de betrokkenen.

Een bijzonder probleem dat wordt aangestipt is de uitzondering in de Belgische wetgeving op de uitoefening van het recht van de burger om toegang te krijgen tot de persoonsgegevens die door strafrechtelijke autoriteiten worden verwerkt. Het uitzonderingsregime waarbij slechts een indirecte toegang wordt verschaft tot de verwerking van persoonsgegevens door de politiediensten, aan de hand van een verificatiesysteem door het Controleorgaan op de politionele informatie wekt frustratie op bij de burger en strookt niet met de transparantieplichting die verwacht wordt van de overheid.

Specifieke aandacht voor kwetsbare groepen. Meer algemeen wordt gepleit voor een bijkomende bescherming voor kwetsbare personen zoals minderjarigen of ouderen door middel van informatie-, sensibiliserings- en vormingsmogelijkheden. De digitale wereld dient laagdrempelig toegankelijk te zijn voor iedereen maar op een geïnformeerde en veilige manier. Dit hangt dan ook samen met de ruimere problematiek van de digitale kloof en het wegwijs maken van kwetsbare groepen in de digitale wereld.

Specifiek wat minderjarigen betreft wordt gewezen op de onduidelijkheid over de wijze waarop de AVG en artikel 7 van de Privacywet dienen te worden toegepast. Artikel 7 van de Privacywet bepaalt dat de verwerking van de persoonsgegevens van een kind met betrekking tot een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind, rechtmatig is indien de toestemming verleend wordt door kinderen van 13 jaar of ouder. De scheidingslijn tussen het gegeven van toestemming in het kader van diensten van de informatiemaatschappij en de rechtsgrond voor de verwerking van persoonsgegevens van minderjarigen buiten dat kader is onduidelijk. Concreet wordt het voorbeeld geschetst van de gezondheidssector. Daar stelt zich de vraag rond de toegang van minderjarigen tot hun gezondheidsgegevens bijvoorbeeld via gezondheidsapps die steeds meer wijdverspreid worden en allerlei diensten aanbieden.

3.8. De rol van de gegevensbeschermingsfunctionaris

Nood aan een grotere privacymaturiteit binnen de organisatie. De centrale rol van gegevensbeschermingsfunctionarissen dient meer visibiliteit te krijgen. Zij zijn een onderdeel in de keten van de verantwoordingsplichting (accountability) in hoofde van een verwerkingsverantwoordelijke of verwerker. Zodoende dragen ze bij tot de interne gegevensverwerkingsprocessen in de vorm van onder andere adviesverlening en toezichtsoopdrachten. Tezelfdertijd vormen zij de brug met de bevoegde toezichtautoriteiten.

Het belang dat binnen een organisatie aan de functie van een gegevensbeschermingsfunctionaris wordt toegekend weerspiegelt het niveau van maturiteit waarmee met gegevensverwerking- en bescherming wordt omgegaan. Er kan echter worden vastgesteld dat nog te weinig beroep wordt gedaan op gegevensverwerkingsfunctionarissen door verwerkingsverantwoordelijken én verwerkers. De rol van de gegevensverwerkingsfunctionaris wordt nog maar al te vaak binnen een organisatie beschouwd als een remmende factor in gegevensverwerkings- of innovatieve processen. Dit ligt deels aan het bestaan van archaïsche organisatieculturen die weinig investeren in change management. Anderzijds bestaat ook nog veel onwetendheid over de rol en het statuut van de gegevensbeschermingsfunctionaris waardoor er niet altijd duidelijk bepaald wordt wanneer en hoe beroep kan of moet gedaan worden op zijn of haar diensten.

Meer flexibiliteit in de wettelijke verplichting tot aanduiding van een gegevensbeschermingsfunctionaris. Het wettelijk kader betreffende de gegevensbeschermingsfunctionaris zou kunnen aangevuld worden om een pooling van gegevensbeschermingsfunctionarissen mogelijk te maken. Er bestaat immers enige bezorgdheid over de mogelijkheid voor kleine organisaties en ondernemingen om te voldoen aan de wettelijke verplichtingen. Het organiseren van een pooling zou hen toelaten beroep te kunnen doen op een gezamenlijke gegevensbeschermingsfunctionaris.

Dit zou hen ook de mogelijkheid geven om te voldoen aan de vereiste van artikel 20 § 2 van de Privacywet die privéorganen verplicht een gegevensbeschermingsfunctionaris aan te stellen indien zij gegevens uitwisselen met de federale overheid. Kleine organisaties en ondernemingen vinden het moeilijk om te voldoen aan deze verplichting en kunnen aldus ongewild geweerd worden uit overheidsopdrachten.

Anderen pleiten er dan weer voor om de verplichting tot het aanstellen van een gegevensbeschermingsfunctionaris uit te breiden en zich niet te beperken tot de gevallen die opgelegd worden door de AVG. Indien de hoofdbezigheid van een organisatie of onderneming bestaat uit het verwerken van persoonsgegevens – ongeacht of het bijzondere categorieën van persoonsgegevens betreft – of indien intrusieve technologieën zoals drones, ANPR camera's of 'augmented reality' applicaties worden ontwikkeld, zou er een gegevensbeschermingsfunctionaris moeten aangeduid worden. Er ontbreekt ook een expliciete rol voor de gegevensbeschermingsfunctionaris in het sociaal recht.

Het terugschroeven van de bijkomende verplichtingen ten opzichte van de AVG. Artikelen 20 § 2 en 21 van de Privacywet worden in vraag gesteld vermits de Belgische wetgever hier verder gaat dan de AVG inzake de verplichtingen om een gegevensbeschermingsfunctionaris aan te stellen. Er wordt gepleit voor de afschaffing van de bijkomende verplichting krachtens artikel 21 van de Privacywet tot het aanstellen van een gegevensbeschermingsfunctionaris door privéorganisaties voor de verwerking van gegevens, afkomstig van de federale overheid, die een hoog risico kan inhouden. De administratieve last ten opzichte van de baten ten aanzien van de bescherming van de gegevens wordt immers als onevenredig ervaren. De overheid beschikt reeds over een gegevensbeschermingsfunctionaris en indien een impactanalyse correct is uitgevoerd worden de risico's verbonden aan de verwerking al op voorhand gemitigeerd.

Wordt deze verplichting toch behouden dan moet op zijn minst de toepassingsvoorwaarden ervan gealigneerd worden met artikel 35 AVG dat minder streng is. Ook de verplichting krachtens artikel 20, § 2 van de Privacywet om een gegevensbeschermingsfunctionaris aan te stellen indien een privéorganisaties persoonsgegevens verkrijgt van een federale overheid moet herbekeken worden. Deze verplichting is immers niet coherent met hetgeen bepaald is in artikel 21 van de Privacywet. Enkel in het geval een privéorganisatie een gegevensbeschermingsfunctionaris heeft aangesteld zou een advies van de beide gegevensbeschermingsfunctionarissen (federale overheid en privéorganisatie) moeten ingewonnen worden voorafgaand aan een gegevensuitwisseling.

Er wordt ook gewezen op de haalbaarheid van sommige verplichtingen of verwachtingen in hoofde van de gegevensbeschermingsfunctionarissen. Zij zijn niet altijd het best geplaatst of uitgerust met de nodige middelen of expertise om bepaalde – soms bijkomende – taken uit te oefenen. Een voorbeeld dat aangehaald wordt is de opdracht voor een gegevensbeschermingsfunctionaris die optreedt binnen het kader van Titel 4 van de Privacywet om een advies te verlenen over het gebruik van de verschillende methoden voor pseudonimisering en anonimisering.

Nood aan samenwerking. In de eerste plaats dient de samenwerking tussen gegevensbeschermingsfunctionarissen ondersteund te worden bijvoorbeeld door het centraliseren van toegang tot expertise, informatie, toepasselijke regelgeving,... Ook de samenwerking tussen de Gegevensbeschermingsautoriteit en de gegevensbeschermingsfunctionarissen verdient verdere aandacht en ondersteuning. Gegevensbeschermingsfunctionarissen zouden moeten kunnen genieten van een beter en direct contact met sectorale experts binnen de Gegevensbeschermingsautoriteit. Er wordt ook gewezen op het belang van een samenwerking tussen de gegevensbeschermingsfunctionarissen en informatiebeheerspecialisten waaronder archivariissen.

Het bestaan van een koepelorganisatie of -organisaties in België zou een bijkomende ondersteuning kunnen bieden in de werkzaamheden van gegevensbeschermingsfunctionarissen. Het zou een platform kunnen zijn om goede praktijken uit te wisselen, standaarden te ontwikkelen en bovenal om in alle discretie een casus te bespreken. Gegevensbeschermingsfunctionarissen zijn immers onderworpen aan het beroepsgeheim waardoor het uitwisselen van informatie slechts onder bepaalde voorwaarden mogelijk is zodat de werkgever van de gegevensbeschermingsfunctionaris niet blootgesteld wordt.

Versterking van het statuut van de gegevensbeschermingsfunctionaris. Er wordt een debat gevoerd over de nood aan bijkomende bescherming voor en versterking van het statuut van de gegevensbeschermingsfunctionaris. Sommigen menen dat de gegevensbeschermingsfunctionaris een statuut gelijkwaardig aan een vakbondsafgevaardigde moet krijgen teneinde zijn rol in volle onafhankelijkheid binnen de organisatie te kunnen uitvoeren.

Anderen menen dat dit niet wenselijk is omdat dit de gegevensbeschermingsfunctionaris in een positie van belangenconflict zou kunnen plaatsen. Er wordt in ieder geval geopperd om een deontologisch kader uit te werken naar analogie van de Franse koepelorganisatie AFCDP.

3.9. Onafhankelijke en efficiënte toezichthoudende autoriteiten

Een vereenvoudiging van het institutionele privacylandschap. Het belang van de onafhankelijkheid van de toezichthoudende autoriteiten en in het bijzonder van de Gegevensbeschermingsautoriteit wordt sterk onderlijnd. Het beheer van persoonsgegevens zowel door de publieke als private sector kan slechts het vertrouwen genieten van de burger voor zover er ook sprake is van een sterke, efficiënte, onpartijdige en onafhankelijke toezichthoudende autoriteit. In dat opzicht wordt erop gewezen dat zowel op wettelijk vlak als in de praktijk dient te worden gesleuteld aan het complexe en versnipperde institutionele privacylandschap. Ook dient de werking van de Gegevensbeschermingsautoriteit te worden bijgestuurd. Het auditrapport van het Rekenhof van 31 mei 2021 wijst in die zin op significante tekortkomingen in de huidige structuur en werking van de Gegevensbeschermingsautoriteit. Een wijziging van de organieke wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit dringt zich dan ook op.

Deze kwestie blijkt een centraal aandachtspunt voor velen. Verwerkingsverantwoordelijken en in het bijzonder overheidsdiensten dienen met een veelheid aan instanties rekening te houden. Dit is het geval om toegang te krijgen tot gegevens (bijvoorbeeld het Rijksregister), gegevens te kunnen doorgeven (bijvoorbeeld het Informatieveiligheidscomité of de Vlaamse Toezichtscommissie) of in het naleven van bepaalde procedurele verplichtingen (bijvoorbeeld de Gegevensbeschermingsautoriteit).

Een bijzonder pijnpunt blijkt de onduidelijkheid over de bevoegdheidsverdeling tussen de verschillende toezichthoudende autoriteiten, zowel interfederaal als interfederaal. Dit zorgt niet alleen voor rechtsonzekerheid, het leidt ook tot onnodige administratieve lasten (bijvoorbeeld de melding van contactgegevens van de gegevensbeschermingsfunctionaris aan meerdere controleautoriteiten) of onduidelijkheid over te volgen procedures (bijvoorbeeld aan welke toezichthoudende autoriteit een gegevenslek gemeld moet worden).

Meer synergiën en samenwerking tussen toezichthoudende autoriteiten. Er is meer afstemming en samenwerking vereist tussen de verschillende toezichthoudende autoriteiten. Het bestaan van meerdere onafhankelijke toezichthoudende autoriteiten heeft immers al geleid tot een aantal aandachtspunten, zoals het ontstaan van divergente interpretaties van de privacywetgeving of praktische moeilijkheden in de modaliteiten voor de uitoefening van inspecties en controles.

Er bestaat een samenwerkingsprotocol tussen de vier federale toezichthoudende autoriteiten maar ten opzichte van de deelstaten en in het bijzonder de Vlaamse Toezichtscommissie ontbreekt dit. De verschillen tussen de toezichthoudende autoriteiten kunnen ook leiden tot een concurrentieel nadeel in de dienstverleningssector ten opzichte van andere Europese landen (bijv. voor direct marketing of cookiebeleid). Er wordt gewezen op het onevenwicht tussen de verschillende beleidsniveaus wat betreft het bestaan van toezichthoudende autoriteiten.

Anderzijds is het institutioneel privacylandschap ook nog niet compleet gelet op de afwezigheid van een onafhankelijk mechanisme dat toezicht houdt op de verwerking van persoonsgegevens door de gerechtelijke autoriteiten. België is door het niet invullen van deze verplichting niet in overeenstemming met de AVG. De specificiteit van het invoeren van een controle op de werking van de gerechtelijke autoriteiten vereist in de eerste plaats echter duidelijkheid over de modaliteiten en de draagwijdte van deze verplichting, in het bijzonder wat betreft de notie “in de uitoefening van gerechtelijke taken”.

Meer middelen voor de toezichhoudende autoriteiten. Er wordt voor gepleit om voldoende middelen toe te kennen aan de toezichhoudende autoriteiten, in het bijzonder om hun ondersteuningsrol voor verwerkingsverantwoordelijken, verwerkers maar ook gegevensbeschermingsfunctionarissen verder te helpen uitbouwen. Zo is er een nood aan praktische richtsnoeren vanwege de Gegevensbeschermingsautoriteit om tegemoet te komen aan vragen en moeilijkheden op het terrein. Dit dient ook de harmonisering van de interpretatie en toepassing van de regelgeving te bevorderen.

Meer algemeen kan een grote discrepantie aan middelen tussen de verschillende toezichhoudende autoriteiten onderling dan wel ten opzichte van intermediaire privacyautoriteiten zoals het Informatieveiligheidscomité een “marktverstoring” effect veroorzaken en aanleiding geven tot een de facto uitbreiding van bevoegdheden.

Meer coherentie en samenwerking met Europese partners. Er wordt ook gepleit voor een nauwere samenwerking tussen de Belgische toezichhoudende autoriteiten en hun Europese en niet-Europese tegenhangers. Verschillen in interpretaties van de Europese standaarden zorgt voor rechtsonzekerheid en dringt de impact van een eengemaakte regelgeving terug.

Een aanpassing van de procedurele bevoegdheden van de Gegevensbeschermingsautoriteit. Er blijkt ook een nood aan het aanpassen van de procedures die van toepassing zijn bij de uitvoering van verschillende bevoegdheden door de Gegevensbeschermingsautoriteit, bijvoorbeeld wat betreft de rechten van verdediging (hoor- en informatieplicht, proceduretermijnen,...).

4. CONCLUSIES EN AANBEVELINGEN

Zoals blijkt uit het vorige hoofdstuk zijn in het kader van de evaluatie van de Privacywet een zeer brede waaier aan opmerkingen, suggesties en verzuchtingen naar voren gekomen. Algemeen blijkt er eensgezindheid over het belang van de Privacywet als centraal regelgevend instrument. De evaluatie heeft echter duidelijk gemaakt dat op sommige vlakken bijsturingen of aanvullingen noodzakelijk zijn.

Sommige van deze vaststellingen overstijgen bovendien het loutere kader van de Privacywet en moeten bekeken worden vanuit het perspectief van de nood aan een werkelijk databeheerbeleid.

Dit is geen opdracht die aan een enkele autoriteit toebehoort. Dit evaluatierapport vertolkt een boodschap voor eenieder die een rol kan spelen in het versterken van de bescherming van de persoonsgegevens van onze burgers en in het voeren van een coherent en adequaat beleid inzake gegevensbeheer.

De aanbevelingen die hieronder opgesomd worden vormen een blauwdruk voor verdere beleidsmaatregelen waarin de federale regering in de eerste plaats haar verantwoordelijkheid zal opnemen. Het betreft een niet-exhaustieve lijst van beleidsmaatregelen die als prioritair moeten worden beschouwd.

Er moet daarbij ook rekening gehouden worden met het Europees kader waarbinnen de Privacywet zich situeert. De mogelijkheden en beperkingen in de toepassing van sommige van deze aanbevelingen zullen moeten afgetoetst worden aan de AVG en in mindere mate de Richtlijn en de Conventie 108(+)

van de Raad van Europa. Meer zelfs, de uitvoering van sommige aanbevelingen kan zich inschrijven in Europese initiatieven, in samenwerkingsverbanden met andere lidstaten van de Europese Unie en kan de gelegenheid zijn voor België om zijn leiderschapsrol te blijven spelen op Europees niveau zoals dat het geval was bij de totstandkoming van de AVG. Anderzijds dient, voor wat betreft de overheidsdiensten, bij de uitvoering van deze aanbevelingen ook rekening te worden gehouden met de specificiteit van de verschillende instellingen en in het bijzonder de politionele en gerechtelijke autoriteiten, de krijgsmacht voor sommige van hun opdrachten alsook de inlichtingendiensten. Deze laatste vallen inderdaad onder aparte gegevensbeschermingsregimes.

In zijn geheel genomen moet deze blauwdruk toelaten om een significante versterking van de bescherming van de privacy van de burger uit te voeren.

TRANSPARANTIE
1. Het aanbrengen van de nodige verduidelijkingen in de Privacywet of het beter kaderen van : ✓ bepaalde concepten en terminologieën zoals de ‘uitoefening van gerechtelijke taken’, ‘doorgifte van persoonsgegevens’, ‘gezondheidsgegevens’, ‘diensten van de informatiemaatschappij’, ‘wetenschappelijk onderzoek’, ‘anonimisering’, het begrip ‘overheidsinstantie’ of de notie ‘verwerkingsverantwoordelijke’; ✓ de mogelijkheid een onderscheid te maken naargelang een verwerkingsverantwoordelijke valt in de categorie van de privésector dan wel publieke sector en onder welke beschermingsregimes (AVG, Richtlijn of andere) een verwerkingsverantwoordelijke valt (op basis van de aard van de autoriteit dan wel naar gelang het type van gegevensverwerking); ✓ bepaalde bijkomende verplichtingen t.o.v. de AVG, bijvoorbeeld in de toepassing van de bepalingen inzake de verwerking van persoonsgegevens van minderjarigen of wat betreft de tussenkomst van de gegevensbeschermingsfunctionaris; ✓ de bruggen tussen de verschillende gegevensbeschermingsregimes naargelang de aard van de verwerkingsverantwoordelijke; ✓ de verhouding ten opzichte van de mogelijks conflicterende concepten of verplichtingen tussen de Privacywet en andere wetgeving en fundamentele rechten (bijvoorbeeld wat betreft het beroepsgeheim, de administratieve openbaarheid of de verhouding tot het strafrecht); ✓ de toepassing van de basisprincipes van het gegevensbeschermingsrecht zodat een duidelijker kader wordt gecreëerd betreffende de verplichtingen voor verwerkingsverantwoordelijken en verwerkers, onder meer betreffende de technische en organisatorische maatregelen, dataminimalisatie en de bewaringstermijnen. Hierbij dient rekening te worden gehouden met bestaande Europese richtlijnen ter zake alsook met de Conventie 108(+) van de Raad van Europa.
2. Het inzetten van middelen om het maatschappelijk debat over privacy te bevorderen. Daarbij moet in het bijzonder aandacht worden besteed aan de verhouding tot andere grondrechten en de ontwikkeling en de impact van nieuwe technologieën, big data, artificiële intelligentie,...

3. Het versterken van de transparantie- en verantwoordingsplicht van de verwerkingsverantwoordelijken. In het bijzonder, wat de overheidsdiensten betreft, moet een centraal kadaster een overzicht bieden van de persoonsgegevens die worden verwerkt, minstens wat betreft verwerkingen die onderworpen zijn aan de AVG. De burger moet ook aan de hand van een digitaal platform toegang krijgen tot zijn persoonsgegevens. Overheidsdiensten moeten ook transparant en evenredig zijn in het gebruik van algoritmes. Daartoe zal een transparantieregister aangelegd worden.
4. Het beter benutten van de ondersteunings- en begeleidingsinstrumenten die de AVG en de Privacywet voorzien. Verwerkingsverantwoordelijken en verwerkers dienen beter in staat te worden gesteld om zich te conformeren naar de geldende privacyregels. De ontwikkeling van meer gedragscodes en certificeringsmechanismen die beter gericht zijn op een specifieke sector (bijvoorbeeld de academische of onderzoekswereld) moet daarin centraal staan. Het belang van de begeleidings-, informatie- en ondersteuningsrol van de toezichthoudende autoriteiten kan daarbij onderstreept worden. Specifieke richtlijnen betreffende het gebruik van privacyimpactanalyses worden ontwikkeld, waar mogelijk in samenwerking met de toezichthoudende autoriteiten.
5. Het ontwikkelen van een digitale identificatieportefeuille waarbij de interactie tussen de burger en privé en publieke instanties op een eenvoudige, laagdrempelige en veilige manier wordt georganiseerd.
6. Het versterken van de uitoefening van de rechten van betrokkenen onder meer door het beter omkaderen van het recht op toegang tot en de overdraagbaarheid van persoonsgegevens. Ook het systeem van indirecte toegang tot persoonsgegevens dat vandaag in België geldt dient te worden herbekeken.

BEHEER VAN GEGEVENS
7. Het versterken in de Privacywet van de basisprincipes van de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, onder meer door het expliciteren dat de essentiële elementen van een gegevensverwerking moeten opgenomen worden in elke reglementering die een verwerking organiseert. Er dient ook duiding en begeleiding te worden voorzien bij de keuze en toepassing van de rechtsgrond voor de verwerking van persoonsgegevens. Aan de hand daarvan dienen de mogelijkheden en grenzen van elke rechtsgrond en van de finaliteit van de gegevensverwerking beter afgebakend te worden.
8. Het aanvullen van de Privacywet met een kader voor de toepassing van de privacyregels in bijzondere situaties zoals een pandemie, crisisbestrijding en humanitaire of andere rampen en dit alles met respect voor de bescherming van de grondrechten en de fundamentele belangen van de burger. Tevens moet de Privacywet worden voorzien van een specifiek wettelijk kader voor de verwerking van bijzondere categorieën van persoonsgegevens, bijvoorbeeld biometrische gegevens.

9. Het voorzien van meer rechtszekerheid en duidelijkheid omtrent de verplichtingen en de gevolgen bij het opzetten van internationale gegevensuitwisselingen met actoren die zich buiten de Europese Unie bevinden. Enerzijds, binnen de grenzen van het Europees kader en onder andere in samenwerking met de andere lidstaten van de Europese Unie zou het rechtskader aangevuld of tenminste verduidelijkt moeten worden, anderzijds dienen er meer ondersteuningsmaatregelen te worden uitgewerkt onder andere voor kleine en middelgrote ondernemingen die niet altijd over de middelen en expertise beschikken om met deze complexiteit om te gaan.
10. Voorzien in een uitdrukkelijk wettelijk kader betreffende het gebruik van ‘regulatory sandboxes’ teneinde verwerkingsverantwoordelijken in staat te stellen proeven van gegevensverwerking in een beveiligde en gecontroleerde omgeving te organiseren.
11. Het ontwikkelen van een globaal databeheerbeleid waarbij niet alleen rekening wordt gehouden met persoonsgegevens maar evengoed maatregelen worden uitgewerkt ten aanzien van rechtspersonen en niet-persoonsgebonden gegevens. In het bijzonder, het ontwikkelen van een beleid en bijhorende instrumenten dat erop gericht is de burger de mogelijkheid te bieden om meer en beter controle over zijn persoonsgegevens uit te kunnen oefenen, bijvoorbeeld aan de hand van datakluisen.
12. Toezien op het wegwerken van de hindernissen ten opzichte van een efficiënte toepassing van de regels inzake gegevensverwerkingen in het kader van wetenschappelijk onderzoek. Een vlotter gebruik van gepseudonimiseerde en geanonimiseerde gegevens moet daarbij centraal staan. In het bijzonder dient het systeem van de derde vertrouwenspartijen te worden versterkt.
13. Het vereenvoudigen van de administratieve mechanismen tot uitwisseling van gegevens tussen overheidsinstanties enerzijds en tussen privé en publieke organismen anderzijds. De toegang tot overheidsgegevens dient op een meer eenvormige, laagdrempelige en pragmatische wijze te worden georganiseerd.

INSTITUTIONELE ACTOREN

14. Het verduidelijken van de verhoudingen tussen de Privacywet, sectorale wetgeving en deelstatelijke wetgeving met een impact op de verwerking van persoonsgegevens enerzijds en de verhoudingen tussen de toezichthoudende autoriteiten anderzijds, onder meer aan de hand van een samenwerkingsakkoord tussen de Federale Staat, de Gemeenschappen en de Gewesten. Een expliciet kader inzake bevoegdheidsverdelingen moet een betere afstemming van beleidsmaatregelen en samenwerking tussen autoriteiten waaronder de toezichthoudende autoriteiten te bevorderen.
15. Het aanpassen van de organieke wetgeving van de federale toezichthoudende autoriteiten. In het bijzonder en met prioriteit dient de onafhankelijkheid en het goed bestuur van de Gegevensbeschermingsautoriteit te worden versterkt. Het auditrapport van het Rekenhof

moet daarin de leidraad vormen. De Gegevensbeschermingsautoriteit moet ten volle haar bevoegdheden kunnen uitoefenen teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de verwerking van hun persoonsgegevens te beschermen en het vrije verkeer van persoonsgegevens te vergemakkelijken. Ook in hun werking en procedures moeten de toezichthoudende autoriteiten bijgestuurd worden teneinde te waarborgen dat zij hun wettelijke opdrachten zo efficiënt en adequaat mogelijk kunnen vervullen en over de nodige slagkracht beschikken om op te treden tegen inbreuken. Principes van vereenvoudiging, rationalisering en het creëren van synergiën zouden daarbij centraal moeten staan. De toezichthoudende autoriteiten zouden ook kunnen profiteren van een sectorale expertise in hun midden. Er zal eveneens een antwoord worden geformuleerd op de verplichting tot het oprichten van een onafhankelijk toezichthoudend mechanisme voor de verwerking van persoonsgegevens door de rechterlijke orde.

16. Meer inzetten op een doeltreffend en gepast handhavingsbeleid in geval van niet-naleving van de privacywetgeving. In het bijzonder moet de toepassing van strafsancities herbekeken en aangevuld worden.

17. Het stimuleren van een brede visie op gegevensbescherming, innovatie en gegevensuitwisseling waarbij wordt vertrokken van de kruisbestuiving tussen verschillende (sectorale) expertisedomeinen, privacy en technologie. Dergelijke visie dient ook geïntegreerd te worden in de structuren en werking van alle belanghebbenden. Een organisatiecultuur die de nodige aandacht besteedt aan het voeren van een privacyconform beleid dient te worden bevorderd. Daartoe dienen de nodige middelen worden vrijgemaakt, zowel op organisatorisch vlak (met de nodige aandacht voor anonimisering bijvoorbeeld) als qua vormingsmogelijkheden. Extern dient in grotere mate gecommuniceerd en gesensibiliseerd te worden over het privacybeleid.

18. Teneinde in te kunnen zetten op het vereenvoudigen van de administratieve mechanismen tot uitwisseling van gegevens zal ook het institutionele landschap moeten aangepast worden aan de hand van duidelijke wettelijke opdrachten die op transparante wijze worden uitgeoefend. In het bijzonder dient de rol en de werking van het Informatieveiligheidscomité te worden aangepast om het databeheerbeleid van de overheid verder te ondersteunen, zonder daarbij afbreuk te doen aan de rol en de bevoegdheden van de toezichthoudende autoriteiten ten opzichte van de beslissingen van het Informatieveiligheidscomité.

19. Het verder uitbreiden van de werking van de dienstenintegratoren zodat zij hun faciliterende opdracht ten aanzien van gegevensuitwisselingen kracht bij kunnen zetten. Daartoe dient ook de toegang tot authentieke bronnen beter omkaderd, vereenvoudigd en uitgebreid te worden. Het opschalen van gegevensuitwisselingen kan ook slechts optimaal verwezenlijkt worden voor zover de toegang tot de authentieke bronnen gratis is.

20. Het uitstippelen van specifieke richtlijnen betreffende de rol, het statuut en de opdrachten van de gegevensbeschermingsfunctionarissen. Aanvullend dient een ondersteuningsbeleid gevoerd te worden om kleinere organisaties in staat te stellen hun wettelijke verplichtingen

na te komen, bijvoorbeeld door de mogelijkheid te bevorderen tot het 'poolen' van gegevensbeschermingsfunctionarissen.