Rapport nr. 2020-02-NL

Burgers en biometrie

Biometrische technieken als toegangscontrole: Wat denkt de burger?

Burgers en biometrie

Biometrische technieken als toegangscontrole: Wat denkt de burger?

Rapport nr. 2020-02-NL

Auteurs: Dormaels Arne, Verwee Isabel, Vanden Hemel Andres
Verantwoordelijke uitgever: Genoe Karin
Uitgever: Vias institute – Dept. Veiligheid en Preventie
Publicatiedatum: 6/01/2020
Wettelijk depot: D/2020/0779/1
Gelieve naar dit document te verwijzen als volgt: Dormaels Arne, Verwee Isabel, Vanden Hemel Andres, Burgers en biometrie – Biometrische technieken als toegangscontrole: Wat denkt de burger?, Brussel, België: Vias institute – Dept. Veiligheid en Preventie
Ce rapport est également disponible en français sous le titre :
This report includes a summary in English.

Inhoudsopgave

Tabellen- en figurenlijst

Samenvatting

De eerste biometrische toepassingen vonden we reeds in de prehistorie. De vingerafdruk werd toen gebruikt voor het bezegelen van commerciële overeenkomsten. Door de opeenvolging van de landbouwrevolutie en de industriële revoluties in de 17e tot 21e eeuw ontstond een automatisering van biometrische technieken. De implementering van deze technieken kende een hoogtepunt naar aanleiding van de aanslagen van 11 september 2001. Er heerst sedertdien een sterk geloof dat door middel van technologie de veiligheid stijgt en de criminaliteit een halt kan toegeroepen worden.

Biometrie heeft betrekking op een verzameling van technieken waarbij lichaamskenmerken van een persoon/individu worden gemeten of vastgesteld. Er bestaan verschillende biometrische technieken; zo wordt er een onderscheid gemaakt tussen fysiologische technieken die betrekking hebben op de natuurlijke verrichtingen van levende wezens en de gedragsmatige technieken die eerder verwijzen naar een activiteit of het gedrag van een individu. Voorbeelden van fysiologische technieken zijn vingerafdrukken, handgeometrie, aderpatroonherkenning, gezichtsherkenning en de irisscan. Voorbeelden van gedragsmatige technieken zijn stemherkenning, klavierscan en handtekeninganalyse. Heel wat van deze technieken kennen een lange geschiedenis. Een automatisering van de biometrische techniek, zoals de vingerafdruk of de irisscan ontstaat vaak als een reactie of een tekortkoming van een andere identificatietechniek.

Het gebruik van biometrische technieken neemt toe in verschillende sectoren. Eén van de hoofdgebruikers betreft de financiële sector en ook in het domein van de migratie wordt biometrie frequent gebruikt. Andere sectoren die dergelijke technologie aanwenden, betreffen overheids- en gezondheidsdiensten, defensie, forensische wetenschappen en de commerciële sector.

Bij de aanwending van biometrische technieken moet men rekening houden met het wetgevend kader. De wetgevende bepalingen van biometrische gegevens worden op internationaal en nationaal niveau geregeld. Op internationaal niveau is de General Data Protection Regulation van toepassing, alsook de wetgeving van de Council of Europe en het Europees Verdrag tot bescherming van de Mens en de fundamentele vrijheden. Op nationaal niveau geldt de Belgische gegevensbeschermingswet en enkele Grondwetsartikelen.

De groeiende aanwending van biometrische technieken en het wetgevend kader leiden tot allerhande discussies. Voorstanders benadrukken de verhoogde efficiëntie en veiligheid terwijl tegenstanders het belang van privacy benadrukken. Principes zoals wenselijkheid, proportionaliteit… worden door critici in de verf gezet en de 'opslag' van de gegevens in een databank is voer voor discussie. Daarnaast zijn er bedenkingen over de implementatie van biometrische technieken en wordt er vaak verwezen naar 'uitspattingen' zoals China bijvoorbeeld, waar verkeersovertreders door middel van gezichtsherkenning worden geïdentificeerd en de foto van de overtreders publiek wordt verspreid. Een cultuur van schaamte wordt op deze manier in de hand gewerkt.

De implementatie van nieuwe technologieën wordt niettemin meer en meer als noodzakelijk beschouwd om zich te beschermen tegen toenemende risico's. Het gebruik van nieuwe technologieën wordt in die zin gelegitimeerd omdat onze samenleving moet beschermd worden tegen ieder denkbaar risico (Vermeersch & De Pauw, 2017). Deze controledrang wordt ook bekritiseerd. Enerzijds waarschuwen verschillende wetenschappers dat de Westerse samenleving in toenemende mate wordt geconfronteerd met een overprotectie, een angstcultuur en de idee dat "nieuwe technologieën nieuwe vormen van surveillantie toelaten, en deze daarom ook moeten worden geïmplementeerd'. Anderzijds spreekt men van de 'silent erosion of privacy' als resultaat van een toenemend gebruik van nieuwe technologieën door private/publieke organisaties en overheden binnen een grijze zone van wetten.

Niettemin stellen we een stijgend gebruik van deze technologieën vast omdat het gebruik ervan niet altijd negatief wordt geconnoteerd. Meer en meer duiken stemmen op die het belang onderschrijven van deze nieuwe surveillancevormen, aldus Vermeersch & De Pauw (2017). Omwille van die reden wordt ook meer en meer onderzoek gevoerd naar het draagvlak en de aanvaardbaarheid van deze technologieën.

Vias institute brengt niet alleen enkele perceptieonderzoeken in kaart – waarbij burgers bevraagd worden omtrent het draagvlak en de aanvaardbaarheid van technologie - maar bevraagt zelf 1000 burgers over de aanwending van biometrische technieken. Kent de burger biometrie? Wat denkt de burger over biometrie? In hoeverre is er een acceptatie van biometrie en hoe groot is deze acceptatie? Wat vindt men over vingerafdrukherkenning als vorm van toegangscontrole? Op welke plaatsen kan vingerafdrukherkenning

worden toegepast? Welke actoren mogen welke vormen van biometrie gebruiken? En quid privacy? Is men bereid privacy in te ruilen voor meer veiligheid?

Een eerste belangrijke vaststelling is dat de kennis varieert naargelang de techniek. De meest gekende biometrische techniek is deze van de vingerafdrukken waarbij maar liefst 85% van de respondenten stelt deze techniek te kennen en te weten wat deze inhoudt. Dit onderzoeksresultaat wordt bevestigd in ander onderzoek (o.a. Krupp, Rathgeb & Busch, 2013; Ada Lovelace institute, 2019). Gelaatsherkenning komt op de tweede plaats, spraak/en stemherkenning op de derde plaats en de minst gekende techniek blijkt de handafdrukherkenning te zijn. Als we kijken naar de achtergrondvariabelen stellen we vast dat de respondenten tussen 18 en 34 jaar vaak meer kennis hebben over deze biometrische technieken en weten wat deze technieken inhouden ten opzichte van andere leeftijdscategorieën.

De kennis over een bepaalde techniek is bovendien fundamenteel voor wat betreft de aanvaardbaarheid ervan. Hoe meer men vertrouwd is met een bepaalde techniek, hoe meer deze wordt aanvaard (Koops & Vedder, 2001; Dinev, Masssimo, Hart, Christian, Vincenzo, 2005). In onze survey blijkt dat de aanvaardbaarheid het hoogst is voor de vingerafdrukherkenning, tevens de meest gekende techniek. De irisherkenning komt op de tweede plaats, handafdrukherkenning op de derde plaats en de vierde plaats is voor de techniek van gelaatsherkenning. De hoogste niet-aanvaardbaarheidsscores vinden we terug bij spraak- en stemherkenning. Het is opvallend dat voornamelijk 55-plussers vingerafdruk- en irisherkenning aanvaarden als vorm van toegangscontrole.

De hoogste bereidwilligheid om de vingerafdruk te gebruiken als vorm van toegangscontrole (81,4%) vinden we terug voor het ontgrendelen van de smartphone. Vervolgens wordt het bedrijf waarin men werkt aangeduid en in derde instantie de luchthaven. De reden waarom het ontgrendelen van de smartphone hoog scoort, heeft wellicht te maken met de frequente toepassing hiervan. Dit is immers een zeer courante praktijk.

Als deze bereidwilligheid gekoppeld wordt aan de achtergrondvariabele 'leeftijd', merken we dat de 18 tot 34-jarigen minder bereid zijn om via vingerafdrukken een toegang te krijgen tot 'het bedrijf waar anderen werken', 'sportclub', 'in een voetbalstadion of dergelijke', 'muziekfestival' en 'onderwijsinstellingen' in vergelijking met de + 34-jarigen. De niet-bereidwilligheid is nog hoger bij 18 tot 34-jarigen voor wat betreft het geven van vingerafdrukken als toegangscontrole tot het 'openbaar vervoer zoals de trein, tram, metro en bus', 'shoppingcentrum' en 'openbare parking'.

De politie mag volgens de respondenten het vaakst technologie en biometrische technieken aanwenden. 81,4% geeft aan dat de politie camera's mag gebruiken, 80,1% vindt dat politie vingerafdrukken mag gebruiken, 59,2% stelt dat dit het geval is voor gelaatsherkenning en volgens 52,6% mag de politie irisscans gebruiken. Dit wordt verklaard door het vertrouwen dat er is in de politie. Er is een verband tussen acceptatie en vertrouwen en onderzoek toont aan dat het vertrouwen in de politie vrij hoog is (Verwee, 2012). Respondenten die publieke autoriteiten vertrouwen zijn sneller geneigd om het gebruik van de technologie door deze autoriteiten te aanvaarden (Vermeersch & De Pauw, 2017; Van den Broek, Ooms, Friedewald, van Lieshout & Rung, 2017; Mitrou, Drogkaris & Leventakis, 2017; Snijders, Biesiot, Munnichs & van Est, 2019; Ada Lovelace institute, 2019). Het publieke belang – zoals het verhogen van de veiligheid of de bescherming – is fundamenteler voor de burger in het acceptatieproces van facial recognition dan het commerciële belang. De burgers zijn minder enthousiast als private bedrijven dergelijke technieken aanwenden. Ze stellen zich meer vragen omtrent de toepasbaarheid, ethiek, privacy, verzameling van data…

De meest sceptische houding voor het aanwenden van de technologie vinden we bij de sociale media. 61% stelt dat de sociale media geen enkele van deze technieken mag aanwenden.

De meerderheid van de respondenten, namelijk 57,5%, is bereid om privacy in te ruilen voor meer veiligheid. De extreme antwoorden scoren lager: men is dus 'eerder wel bereid' of 'eerder niet bereid' om privacy in te ruilen voor meer veiligheid. Als we deze resultaten kruisen met de vraag naar aanvaardbaarheid zien we dat de respondenten die biometrische technieken aanvaarden, meer bereid zijn om privacy in te ruilen voor veiligheid. Dit impliceert dat degene die de techniek niet aanvaarden doorgaans minder (of niet) bereid zijn om privacy in te ruilen voor veiligheid. Aangaande privacy en veiligheid is het tot slot belangrijk dat Europees onderzoek (Pavone, Santiago & Degli-Esposti, 2015) stelt dat dit een 'en-en'- in plaats van een 'of-of'-verhaal is waarbij burgers privacy én veiligheid wensen.

1 Inleiding

De technologische ontwikkelingen gaan bijzonder snel. Computers, smartphones en internet zijn centrale aspecten van het dagelijkse leven (Kalyani, 2017) en ze zijn een evidentie geworden. De keerzijde van de medaille is dat deze technologische vooruitgang ook opportuniteiten voor criminelen genereren waardoor er meer geavanceerde en gesofisticeerde inbreuken op veiligheid plaatsvinden. Om ons hiertegen te wapenen nemen allerhande vormen van beveiliging toe, alsook de toepassing van biometrische technieken.

Het begrip biometrie valt uiteen in twee concepten, 'bios' en 'metrie', waarbij het eerste verwijst naar 'levend' en 'metrie' naar 'meten' (Maguire, 2009). Biometrie betreft met andere woorden een verzameling van technieken waarbij lichaamskenmerken van een individu worden gemeten of vastgesteld. Men kan hierbij bijvoorbeeld denken aan vingerafdrukken. Een vingerafdruk is een biometrisch spoor die valt terug te leiden tot één individu.

Door middel van biometrische technieken worden biometrische gegevens geverifieerd. Biometrie won meer aan meer aan belang in de strijd tegen fraude en bij persoonsidentificatie. De idee dat de implementatie van biometrische technologie een veilige samenleving genereert, kent een hoogtepunt bij de aanslagen van 11 september 2001. Na deze aanslagen werd biometrie gehanteerd in de strijd tegen terrorisme. Door gebruik te maken van biometrie kunnen gevoelige ruimtes beter worden beveiligd en kan men zich beter te beschermen tegen identiteitsdiefstal (een problematiek die gelinkt wordt aan terrorisme). Het verlies of diefstal van toegangsbadges kan op deze wijze eveneens worden geëlimineerd.

In het eerste deel van dit rapport wordt de werking van verschillende technieken besproken. Er wordt een onderscheid gemaakt tussen de fysiologische technieken - zoals de vingerafdrukken, handgeometrie, gezichtsherkenning en de irisscan - en de gedragsmatige technieken, zoals stemherkenning, klavierscan en handtekeninganalyse. Per techniek worden enkele voor- en nadelen opgesomd. Vervolgens wordt er ingegaan op de sectoren die in hoofdzaak gebruik maken van biometrische technieken. Een beknopt juridisch kader wordt beschreven en enkele meer algemene kritische reflecties komen aan bod.

Het tweede deel van dit onderzoeksrapport gaat in op de publieke opinie inzake biometrische technieken. Op basis van een literatuurstudie worden verschillende factoren opgesomd die de publieke opinie over technologie beïnvloeden. Er worden in onderzoek vaak bepaalde frames gehanteerd om deze opinie te bestuderen. Verder wordt ingegaan op de acceptatie van technologie in de slimme stad en de acceptatie van technologiegebruik door de politie.

Quid België? Vias institute bevroeg duizend Belgen over hun kennis en acceptatie van biometrische technieken. Uit de resultaten van (inter)nationaal onderzoek blijkt dat vingerafdrukken de meest gekende en aanvaarde vorm binnen biometrie is. Om deze reden werd in de bevraging dieper ingegaan op de vingerafdrukken. Meer bepaald werden verschillende locaties (bijvoorbeeld: het bedrijf waar men werkt, in een voetbalstadion of dergelijke, op een muziekfestival, op de luchthaven,…) voorgelegd en gevraagd in hoeverre respondenten bereid zijn om vingerafdrukken te gebruiken als toegangscontrole. Vervolgens werd gepeild naar een aantal stellingen, bijvoorbeeld "*mag politie meer gebruik maken van vingerafdrukken of camera's dan andere sectoren?*". Tot slot wordt gepeild naar de mate waarin respondenten bereid zijn om privacy in te ruilen voor meer veiligheid. De resultaten worden besproken in het licht van de (inter)nationale onderzoeksbevindingen.

2 Biometrische technieken

In dit hoofdstuk komen de verschillende biometrische technieken aan bod. Allereerst wordt de algemene historiek besproken, om vervolgens de biometrische technieken toe te lichten.

2.1 Korte historiek

In deze algemene historiek van de biometrie wordt verwezen naar enkele noemenswaardige wetenschappers. Adolphe Quetelet (1820) wordt beschouwd als de grondlegger van de antropometrie, de toegepaste antropologie, een wetenschap waarin het meten van mensen centraal staat (Eknoyan, 2007). Hij paste als één van de eersten statistische methoden toe in de sociale wetenschappen. In zijn werk 'De gemiddelde mens' bestudeerde hij namelijk de gemiddelde waarden van lichaamsmaten. Een tweede vermeldenswaardige figuur is Alphonse Bertillon (1880). Als directeur van de afdeling identificatie bij de politie bouwde hij verder op de antropometrie. Bertillon ontwikkelde een techniek om recidivisme bij verdachte criminelen op te sporen. Hij deed dit door een tiental lichaamskenmerken, zoals het hoofd en de vinger, nauwkeurig op te meten en op basis hiervan een uniek beeld van het individu te creëren. Enkele jaren later werden bij deze techniek ook foto's gebruikt. Door de opkomst van de dactyloscopie waarbij mensen werden geïdentificeerd aan de hand van vingerafdrukken verdween Bertillons' systeem (Augustyn, Bauer, Duignan, Eldridge, Gregersen, Luebering, McKenna, Petruzzello, Rafferty, Ray, Rogers, Tikkanen, Wallenfeldt, Zeidan & Zelazko, 2019).

Een laatste noemenswaardige figuur binnen de biometrie is August Comte (1815), de grondlegger van het positivisme. Binnen deze stroming linken een aantal empirische wetenschappers het concept 'misdadigheid' aan de menseigen kenmerken van individuen (Beirne, 1987). Dit deed ook Lombroso. Door zijn werk 'L'uomo Delinquente' of 'de geboren crimineel' won de biologie aan belang in de twintigste eeuw. Het werd na de tweede wereldoorlog echter ondenkbaar dat de lichaamskenmerken van de mens werden bestudeerd om hieruit bepaalde conclusies te trekken. Dit was voornamelijk te wijten aan de praktijken van Nazi-Duitsland, waarin de lichaamskenmerken van bepaalde bevolkingsgroepen in kaart werden gebracht om deze te onderscheiden van onder meer de Duitsers, met alle gevolgen van dien (Lauryssen, Vander Beken, Hebberecht & Pauwels, 2014).

2.2 Welke biometrische technieken bestaan er?

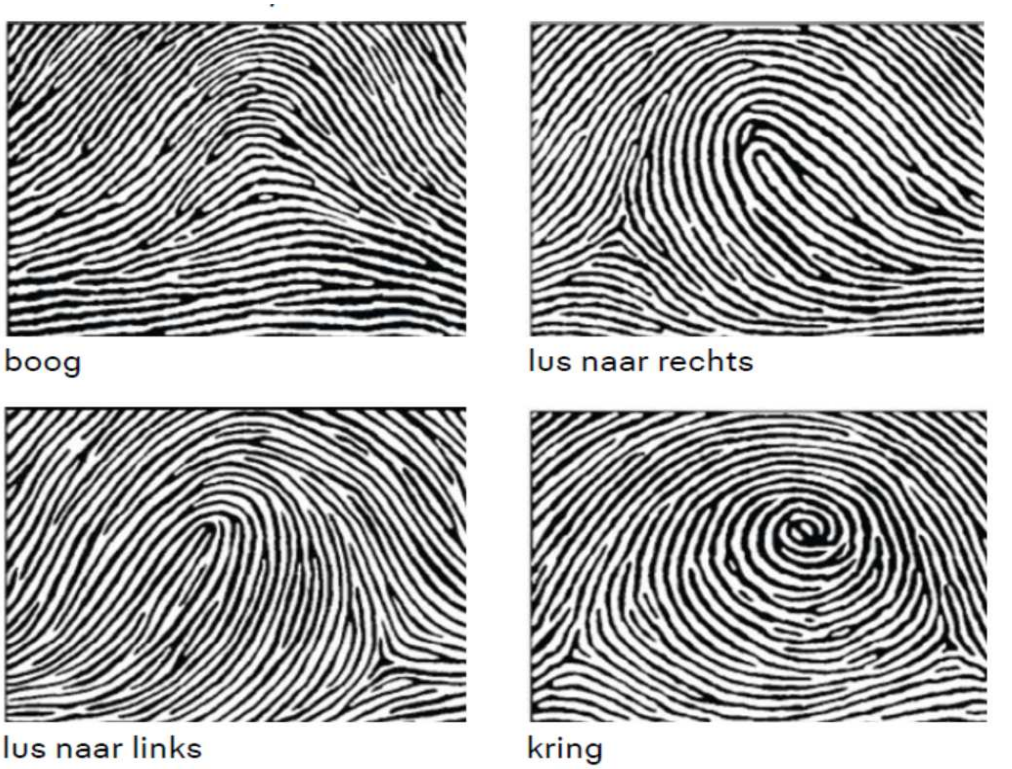
Biometrie betreft een vorm van toegepaste wetenschap waarbij men de bron probeert te achterhalen van het aangetroffen spoor (Broeders & Muller, 2008). Bij de beschrijving van de verschillende biometrische technieken wordt een onderscheid gemaakt tussen fysiologische en gedragsmatige biometrische gegevens. 'Fysiologisch' wijst op bepaalde uiterlijke kenmerken van levende wezens, zoals bijvoorbeeld de vingerafdruk (Ensie, 2019), en 'gedragsmatig' betreft eerder een activiteit of gedrag van een individu, zoals stemherkenning (Van den Boogaerde, 2006).

2.3 Fysiologische technieken

2.3.1 Vingerafdrukherkenning

2.3.1.1 Werking

Vingerafdrukherkenning is gebaseerd op de unieke, complexe en blijvende morfologische structuur van de papillair lijnen (Riemen & Voorhoeven, 2015). De genetische- en omgevingsfactoren verklaren de natuurlijke variatie aan vormen en details in de papillair lijnen. Zo vindt men bij identieke tweelingen geen exact gelijk papillair lijnenbeeld.



Figuur 1 Verschillende vormen van papillair lijnen

Elke vinger bovendien heeft verschillende vormen van papillair lijnen. Om de unieke structuur van de vinger te analyseren, kan gekeken worden naar verschillende niveaus. Op een eerste niveau wordt gekeken naar de evenwijdigheid van de lijnen. Op basis van dit niveau wordt gesproken over een boog, lus of kring. Vervolgens wordt de loop bestudeerd en als laatste wordt gekeken naar de vorm van de lijnranden, de breedte van de lijnen en de vorm en ligging van de poriën (Riemen & Voorhoeven, 2015).

2.3.1.2 Toepassing

Verenigde Staten

De FBI ondernam sinds 1930 pogingen tot de oprichting van een nationale databank met biometrische gegevens. Sinds 1975 werd dit proces geautomatiseerd en werden de vingerafdrukken bijgehouden in het Automated Fingerprinting Identification System (AFIS) (Varenna, 2011). Er was daarnaast nood aan een betere identificatie en authenticatie. Deze biometrische identificatie werd gezien als oplossing in de strijd tegen terrorisme, illegale migratie en cybercriminaliteit. Startend onderzoek van de FBI, Binnenlandse zaken en politieambtenaren in landen zoals Japan en Frankrijk, zorgde voor de ontwikkeling van de AFIS-databank (N.d., 2018). De databank is sindsdien wijdverspreid en wordt in veel landen gebruikt, onder meer in België, Canada, Denemarken en Turkije. Naast deze algemene databank bestaat er een diversiteit aan nationale databases, bijvoorbeeld het NAFIS-systeem (National Automated Fingerprint Identification System) in Australië. AFIS evolueert tegenwoordig richting ABIS (Automated Biometric Identification System) door de ontwikkeling van nieuwe biometrische technologieën zoals iris- en gezichtsherkenning (N.d., 2018).

Verenigde Naties

De Verenigde Naties ontwikkelden een besluit over biometrie in 2016 omtrent het versterken van internationale wetshandhaving en justitiële samenwerking in de strijd tegen terrorisme. In dit besluit staat dat de lidstaten systemen moeten ontwikkelen voor het verzamelen van biometrische gegevens om terroristen en terroristische netwerken te identificeren. Door dit besluit werd een project opgestart over het gebruik van biometrie en werd het delen van biometrische gegevens versterkt. Het project werd geïmplementeerd door het Counter-Terrorism Committee Executive Directorate (CTED), The Counter-Terrorism Implementation Task Force (CTITF), INTERPOL, the United Nations Office on Drugs and Crime (UNODC), the International Civil Aviation Organization (ICAO) en the United Nations High Commissioner for Refugees (UNHCR).

Ten slotte is er sinds 2017 een Visa Informatie Systeem (VIS). Dit systeem maakt de uitwisseling van visumgegevens mogelijk tussen de Schengenlanden. Het VIS bestaat uit een centraal computersysteem dat gekoppeld is aan nationale informaticasystemen van overheden en consulaten. Het gebruikt onder meer vingerafdrukken om te kijken of iemand een geldig visum heeft en vereenvoudigt het behandelen van asielaanvragen. De bedoeling is dat dit systeem tegen 2020 op punt zal staan, aldus de Gegevensbeschermingsautoriteit of GBA (Gegevensbeschermingsautoriteit, 2018).

Europa

Op Europees niveau kwam er eveneens meer aandacht voor het gebruik van biometrie. In 2003 werd Eurodac opgericht, in navolging van het Dublin akkoord uit 1990. Eurodac is een vingerafdrukkendatabank in het kader van migratie. Deze databank laat toe om vingerafdrukken te vergelijken en helpt bij de bepaling van welke lidstaat bevoegd is voor het behandelen van een asielaanvraag. De wetgevingsautoriteiten en Europol kunnen deze vingerafdrukken vergelijken binnen onderzoek, enkel met als doel preventie, detectie of onderzoek van ernstige criminaliteit of terrorisme. Daarenboven zijn opzoekingen aan strikte voorwaarden gekoppeld: zo moet de vingerafdruk bijvoorbeeld eerst in alle andere mogelijke databanken doorzocht worden (Europese Commissie, 2019).

Naast Eurodac is er sinds 2005 het verdrag van Prüm. Dit verdrag werd afgesloten tussen België, Duitsland, Frankrijk en Luxemburg. In deze overeenkomst werden afspraken gemaakt omtrent de uitwisseling van data op het gebied van DNA, vingerafdrukken en verkeersgegevens met als doel de strijd tegen terrorisme en illegale migratie aan te gaan, en een eenvoudigere politie- en justitiesamenwerking (Van den Boogaerde, 2006).

Daarnaast wordt op het Europees niveau het 'entry-exit system' ontwikkeld, met als doelstelling het ontplooien van sterkere en slimmere grenscontroles. Dit systeem moet operationeel zijn tegen 2020 en zou ook biometrische gegevens gebruiken (Europese Commissie, 2016).

UK

Op het nationaal niveau vinden evenzeer initiatieven plaats om nationale databases te maken. In het Verenigd Koninkrijk wordt van alle personen die een asielaanvraag indienen een vingerafdruk en foto genomen en deze worden bewaard in een database. Tijdens deze aanvraag wordt in de nationale politiedatabank (IDENT1) gezocht naar het criminologisch verleden van de asielaanvrager (Houses Of Parliament, 2018).

Nederland

In Nederland is de overheid sinds 2007 gestart met de ingebruikname van de vingerafdruk als identificatiemiddel op een paspoort of identiteitskaart.

België

Sinds de aanslagen in Parijs (2015) en Brussel (2016) werd ook door de Belgische regering een akkoord gevormd om op de elektronische identiteits- en vreemdelingenkaarten twee vingerafdrukken te bewaren om identiteitsfraude tegen te gaan. Dergelijke fraude wordt vaak gebruikt in terrorisme en mensenhandel. In 2018 gaf de voormalige Privacycommissie (Nu GBA) een negatief advies over deze maatregel. De maatregel werd als 'overmatig' gezien en niet conform met de algemene verordening van gegevensbescherming, omdat het gebruik van vingerafdrukken op identiteitskaarten niet verplicht wordt volgens de Europese wetgeving, in tegenstelling tot bijvoorbeeld paspoorten. Ondanks het negatieve advies van de GBA werd het voorstel goedgekeurd, met als gevolg dat vanaf april 2019 op elke identiteitskaart een vingerafdruk van de linker- en rechterwijsvinger op de chip wordt opgeslagen (Belga, 2018). De Liga voor Mensenrechten reageerde afwijzend en stelde dat de voornaamste reden voor invoering, namelijk de stijging van identiteitsfraude, een verwaarloosbaar argument is. Daarnaast stelde zij dat er al een foto op de identiteitskaart staat, dat er geen rekening wordt gehouden met potentiële risico's voor de burgers en dat de basisprincipes van de nieuwe privacywetgeving worden genegeerd. Kortom: de Liga acht de maatregel niet proportioneel en gelooft dat hiermee het belang van privacy wordt ondergraven (Belga, 2018).

Inmiddels werd deze invoering van de vingerafdruk uitgesteld en liep de uitrol van de door de kamer goedgekeurde wet van Michel I vertraging op omdat de regering in lopende zaken ging eind 2018 (Belga, 2019). De woordvoerder van bevoegd minister De Crem verklaarde dat de beslissing niet wordt teruggedraaid: "*De achterstand heeft niets met drukkingsgroepen te maken, enkel met de situatie van lopende zaken. We voeren de regeringsbeslissing uit*", aldus Eenaerts. Volgens de Vlaamse Vereniging van Ambtenaren en Beambten Burgerlijke Stand vzw wordt dit uitgesteld tot na de zomervakantie 2019 en zal dit naar verwachting worden opgestart midden september 2019 (Vlavabbs, 2019). De opstart gebeurt door middel van een

proefproject waarbij verschillende steden en gemeenten de vingerafdruk op de identiteitskaart laten plaatsen. De vingerafdrukken komen op de eID terecht maar zullen nog niet te vinden zijn in een algemene databank. In deze databank blijven de vingerafdrukken drie maanden beschikbaar. Dobbelaere-Welvaert stelt kritisch dat het niet duidelijk is wie de gegevens verwerkt, welk systeem steden en gemeenten krijgen, wie toegang heeft tot deze databank en ook de meerwaarde van deze wet as such wordt nog steeds in twijfel getrokken door Dobbelaere-Welvaert (Dobbelaere-Welvaert, 2019).

2.3.1.3 Voor- en nadelen vingerafdruk

Eén van de grootste voordelen van het gebruik van biometrische gegevens is de eenvoudige manier waarop mensen kunnen worden herkend. Biometrie wordt beschouwd als een erg accurate en betrouwbare manier van identificeren (Veridin, 2019). Het belangrijkste voordeel van de vingerafdruk is dat het een uniek lichaamseigen kenmerk is dat vrij onveranderlijk is doorheen de levensjaren. Het meten van een vingerafdruk is bovendien één van de goedkopere biometrische technieken (Heukers, 2006). Badges of toegangscodes worden wel eens vergeten, echter biometrische gegevens – zoals een vingerafdruk – heeft men altijd bij zich. Het gebruik van biometrie bemoeilijkt identiteitsdiefstal en komt tegemoet aan tekortkomingen van andere vormen van toegangscontrole. Zo is recent gebleken dat toegangsbadges op een eenvoudige manier kunnen worden gekopieerd door middel van een simpel Radio-Frequency Identification (RFID) kopieertoestel (Standaert, 2019).

Eén van de grootste nadelen is dat de biometrische gegevens gestolen kunnen worden en dit levenslange gevolgen kan hebben. Een wachtwoord kan men veranderen en een badge deactiveren, maar dit is bij een vingerafdruk onmogelijk. Biometrische gegevens – en de opslag van data – kunnen misbruikt worden door allerhande actoren, bijvoorbeeld een verzekeringsmaatschappij. Zo kan men het medisch verleden van een persoon snel controleren en op basis daarvan beslissen of men de persoon in kwestie al dan niet verzekert (Debeuckelaere, 2008). Tot slot beschouwen burgers het geven van biometrische gegevens frequent als een schending van hun privacy (Dobbelaere-Welvaert, 2019; El-Abed, Giot, Hemery & Rosenberger, 2012) en zette dit aan tot bewegingen zoals 'stop de vingerafdruk'. Sceptici stellen dat het nemen van een vingerafdruk een schending van de privacy impliceert en het opslaan van deze data gevaarlijk is voor misdoeleinden. Voorts hebben biometrische systemen een hoge kostprijs: hoe geavanceerder de techniek, hoe hoger de prijs.

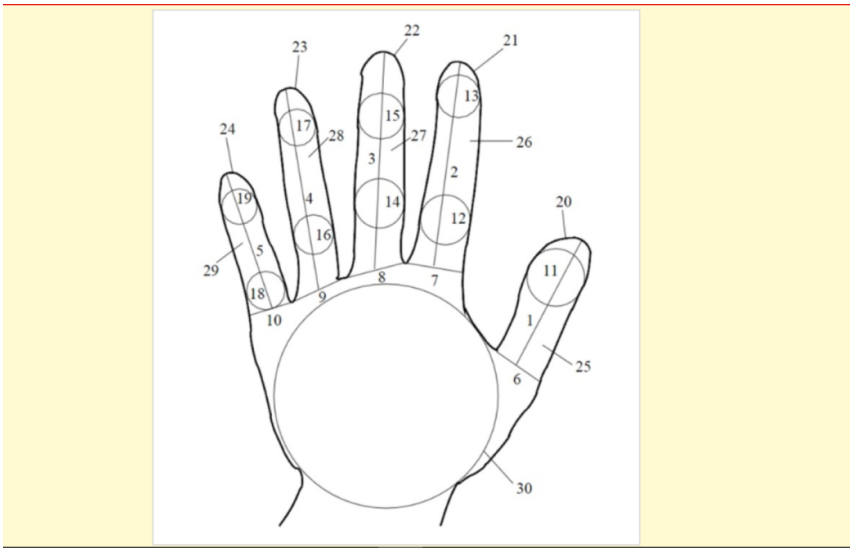
Een ander nadeel van vingerafdrukherkenning is dat het sporen achterlaat, in tegenstelling tot bijvoorbeeld aderpatroonherkenning. Ook bezit 4% van de bevolking onvoldoende waarneembare vingerafdrukken (Thakkar, 2018). In het kader van toegangscontrole kan dit een belemmering zijn, want wat gebeurt er met personen die geen vingerafdruk kunnen afstaan? Wordt bij hen de vingerafdruk vervangen door een badge? Zo werkt de loutere aanwezigheid van onderscheidbare groepen ingroup-favoritisme in de hand en kunnen vooroordelen en discriminatie ontstaan ten aanzien van de andere of outgroup (bijvoorbeeld personen met een badge) (Tajfel, 1974). Daarnaast werkt de techniek niet altijd even snel en treden soms fouten op doordat de vinger niet goed op de scanner wordt geplaatst. Het is bovendien een techniek die 'spoofing' (namaak) toelaat (New York Times, 2017). Tot slot heeft de vingerafdruk het nadeel dat bacteriën en virussen sneller verspreid kunnen worden (Deurplus, 2019).

Belangrijk nadeel bij vingerafdrukherkenning bij misdrijven is ook de interpretatie tussen spoor en referentie. Stel men vindt een vingerafdruk op het wapen dat is gebruikt bij een moord en men wil weten of de vingerafdruk afkomstig is van de verdachte. Het spoor op het wapen wordt vergeleken met de vingerafdrukken van de verdachte. Dit proces verloopt niet automatisch, er komt immers interpretatie bij kijken. Het gevaar van bias (of denkfouten) bestaat wanneer de expert teveel context informatie ontvangt en zich daardoor mogelijk beperkt tot het zoeken naar bevestigende informatie (confirmation bias) met mogelijk grote gevolgen. Dit werd onder meer vastgesteld in een experiment van Dror naar aanleiding van de aanslagen in Madrid (Kassin, Dror & Kukucka, 2013).

2.3.2 Handgeometrie

2.3.2.1 Werking

Handgeometrie is gebaseerd op een beeld van de hand dat gevormd wordt door een digitale camera. Er wordt daarbij voornamelijk gekeken naar de lengte van de vingers, de dikte en de locaties van de op de figuur aangegeven punten (NSTC Subcommittee On Biometrics, 2006).



Figuur 2: Handgeometrie bron

Bij de afname wordt een 3D-print van de hand gemaakt om deze te vergelijken met 90 herkenningspunten. Daardoor wordt de techniek in hoofdzaak gebruikt voor verificatie en niet voor identificatie (Thakkar, 2018).[1] Het gebruik van handgeometrie is wijdverspreid in de Verenigde Staten, maar iets minder bekend in Europa (Van den Boogaerde, 2006).

2.3.2.2 Voor- en nadelen handgeometrie

Het belangrijkste voordeel bij handgeometrie is dat de techniek snel en makkelijk is in gebruik. Het is daarenboven minder indringend, omdat de vorm van de hand door anderen wordt waargenomen. Dit wordt als minder ingrijpend beschouwd dan een effectieve vingerafdruk. Daarnaast speelt, in tegenstelling tot bijvoorbeeld de vingerafdruk, de conditie van de huid geen rol. Littekens, verbrande vingers of vuil hebben geen invloed op dit systeem (tenzij zwellingen ontstaan of andere aandoeningen waardoor ook de geometrie van de handen wordt aangetast). Het is bovendien een techniek die zich niet makkelijk laat namaken (Thakkar, 2018).

Nadelig aan handgeometrie is dat de geometrie van de handen niet zo uniek is en bijgevolg niet toepasbaar is in situaties die een hoge beveiliging vereisen. Daarnaast is het een dure techniek, aangezien gewerkt wordt met een 3D-print. Zo zou een vingerafdruksysteem al verkrijgbaar zijn vanaf 56 euro, terwijl een systeem van handgeometrie snel meer dan 1000 euro kost, aldus Thakkar (2018).

2.3.3 Aderpatroonherkenning

2.3.3.1 Werking

Binnen de aderpatroonherkenning bestaan er verschillende technieken. Ten eerste is er de handpalm-aderpatroonherkenning dat het aderpatroon in de handpalm herkent. Een tweede vorm betreft de vinger-aderpatroonherkenning, een meer compacte techniek omdat een kleiner oppervlak wordt gescand. Dit is echter minder gebruiksvriendelijk omdat er minder referentiepunten zijn. Naast de aderpatroonherkenning in de handen en vingers kan deze techniek ook worden toegepast op het menselijk netvlies (retina). Elke retina heeft immers een complexe en unieke structuur van haarvaten en doorbloeding (Recogtech, 2019).

Het fundament van deze technieken is echter steeds gelijk. De hemoglobine in het bloed bevat zuurstof bij het transporteren naar de weefsels in het lichaam. Zuurstofarme hemoglobine absorbeert infrarood licht, waardoor het aderpatroon zichtbaar wordt aan de hand van infraroodstralen.

[1] 'Identificeren' betekent het bevestigen of weerleggen van de identiteit van een persoon op basis van biometrische gegevens. Bij 'verificatie' daarentegen is de identiteit van de persoon gekend, en dient de techniek om te bevestigen of te weerleggen of de persoon is wie hij of zij beweert te zijn.

2.3.3.2 Voor- en nadelen aderpatroonherkenning

De techniek van aderpatroonherkenning is moeilijker na te maken dan bijvoorbeeld deze van de vingerafdruk. Het is een veiligere techniek dan vingerafdrukherkenning omdat het gaat over onderhuidse informatie. Tevens werkt de techniek sneller en is het gebruiksgemak groter dan bij vingerafdrukken.

Een belangrijk nadeel van aderpatroonherkenning is dat de techniek duurder is dan bijvoorbeeld vingerafdrukherkenning (Recogtech, 2019). Daarnaast heeft de temperatuur een belangrijke invloed aangezien het patroon van de aderen wordt geanalyseerd. Zo zijn heel koude vingers niet of heel moeilijk te lezen met behulp van aderpatroonherkenning. Ook personen met het syndroom van Raynaud, waarbij bloedvaten in de vingers en tenen tijdelijk worden afgesloten of vernauwd, kunnen problemen ondervinden met aderpatroonherkenning (Recogtech, 2019).

2.3.4 Gezichtsherkenning

2.3.4.1 Werking

Gezichtsherkenning kan gebeuren aan de hand van een foto of infraroodstralen van het gezicht. In het eerste geval wordt er een foto genomen van het gezicht en vergeleken met een bestaande foto. Wanneer er met infraroodstralen wordt gewerkt, worden sensoren ingebouwd in het systeem die vervolgens een 3D-scan maken van het gezicht. Hierbij worden honderden punten in kaart gebracht zodat de unieke verhoudingen - zoals de afstand tussen de ogen, mond, neus en oren - achterhaald kunnen worden (Peeters, 2019).

2.3.4.2 Voor- en nadelen gezichtsherkenning

Het voordeel van gezichtsherkenning is dat de vereiste menselijke interventie minimaal is. De voortdurende ontwikkeling van technologie speelt een centrale rol in dit verhaal. De continue verbetering van de camera's zorgt voor een kwaliteitsvoller beeld van het gezicht, en bijgevolg voor een nauwkeurigere gezichtsherkenning. De technologie maakt het eveneens mogelijk om de gezichtsherkenning gesofisticeerder te maken, zo ontwikkelen onderzoekers bijvoorbeeld systemen die bewegende gezichten herkennen. Daarnaast kan zelfs in het donker een beeld van het gezicht worden gemaakt aan de hand van infrarood gezichtsherkenning (Peeters, 2019).

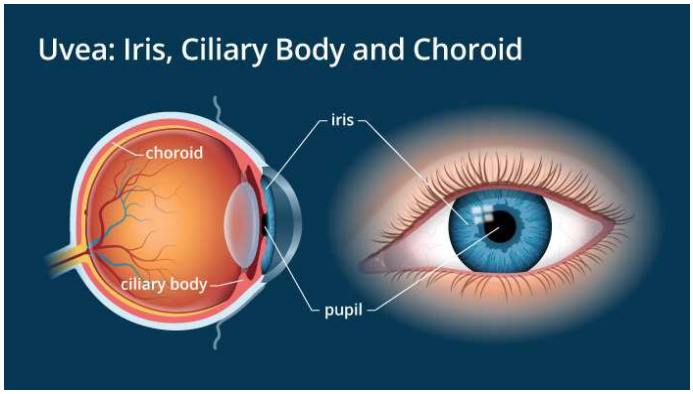
Een nadeel van gezichtsherkenning zonder infrarood, is dat er geen beeld kan worden gemaakt van een gezicht in het donker (Peeters, 2019). Daarnaast wordt de gezichtsherkenning in het algemeen als een gevaarlijkere techniek beschouwd in vergelijking met andere vormen. De gegevens die nodig zijn voor de gezichtsherkenning zijn eenvoudig op het internet te vinden, veel mensen zijn immers een tiental of zelfs honderden tot duizenden keren gefotografeerd. Door de technologische ontwikkelingen en mediakanalen zijn deze foto's eenvoudig te raadplegen op het internet, en kunnen deze bijgevolg makkelijk van op afstand worden gebruikt zonder toestemming van de betrokken persoon. Dit in tegenstelling tot andere soorten toegangscontrole zoals de vingerafdruk die moeilijk te verkrijgen is zonder toestemming (Elgan, 2017).

2.3.5 De irisscan

2.3.5.1 Werking

De irisscan is gebaseerd op de werking van een Charge-Coupled Device (CCD)-camera. Een CCD is een chip die elektromagnetische straling omzet in elektrische lading. Zo wordt het opgevangen licht omgezet in een elektrisch signaal, dat vervolgens door een chip wordt omgezet in binaire codes die door de computer begrepen kunnen worden (N.d., 2016).

Bij dit beeld wordt de iris gelokaliseerd. Vervolgens wordt gekeken naar de buiten -en binnenranden van de iris. Op deze manier wordt de plaats van de iris en het oogwit heel nauwkeurig bepaald (Fig 3).



Figuur 3: Uvea

2.3.5.2 Voor- en nadelen irisscan

Voordelig aan de irisscan is dat de unieke structuur van de iris niet genetisch bepaald is en dat bijgevolg ogen met dezelfde genetische eigenschappen ook verschillende irissen hebben. De iris is door een vlies beschermd tegen slijtage en verandert nauwelijks. Dit in tegenstelling tot bijvoorbeeld de vingerafdruk, die heel gevoelig is voor veranderingen (N.d., 2016). Ook blinde personen kunnen door een irisscanner herkend worden als zij een iris hebben. Het is tevens een techniek waarmee moeilijk te frauderen valt (Van den Boogaerde, 2006). De irisscan wordt daarom vaak gebruikt op plaatsen die sterk beveiligd worden.

Deze techniek heeft echter ook enkele nadelen. De iris bestaat uit enkele millimeters wat herkenning op lange afstand onmogelijk maakt. De iris is bovendien een bewegend doelwit waardoor het in beeld brengen ervan niet evident is. Bij Aziatische personen is de iris vaak verborgen. Het betreft ook een weinig gebruiksvriendelijke techniek en velen ervaren een scan van de ogen als storend. De hygiëne wordt tot slot als een storende factor beschouwd, omdat men de kin op een houder moet plaatsen bij het scannen (El-Abed, Giot, Hemery & Rosenberger, 2012)

2.4 Gedragsmatige technieken

2.4.1 Stemherkenning

2.4.1.1 Werking

Stemherkenning kan zowel onder de behaviometrics als onder de fysiologische biometrics worden geplaatst. Stemherkenning gaat over het herkennen van stemmen, en mag niet verward worden met spraakherkenning. Deze laatste betreft de mogelijkheid van een systeem om zowel vast te stellen als te verwerken wat een persoon zegt. Die techniek wordt vaak gebruikt om gesproken tekst om te zetten naar geschreven tekst.

Bij stemherkenning wordt een spraakmonster vergeleken met een opgeslagen ‘stemafdruk’. Deze herkenningssystemen kunnen tekst-afhankelijk of tekst-onafhankelijk zijn. Bij tekst-onafhankelijke systemen worden de unieke vocale kenmerken van een individu afgeleid, dit in tegentelling tot tekst-afhankelijke systemen, waarbij ook wat de persoon zegt een invloed heeft (Stellar Business Computing, 2018).

2.4.1.2 Voor- en nadelen stemherkenning

Een voordeel van stemherkenning is dat deze techniek in vergelijking met andere biometrische systemen relatief goedkoop is. Deze methode is bovendien nauwkeurig. Zo hebben identieke tweelingen een unieke klank, toonhoogte en frequentie. Ten slotte krijgt dit systeem vaak de voorkeur van burgers, omdat het contactloos kan en niet opdringerig is.

Nadelig aan het gebruik van stemherkenning is de mogelijke geluidshinder. Anderzijds kan het bij langdurig en veelvoudig gebruik van de stem zorgen voor stembandklachten. Het gebruik van stemvervormers kan de stemherkenning bemoeilijken.

2.4.2 Klavierscan

2.4.2.1 Werking

Bij de klavierscan wordt de snelheid van het typen bekeken, de dynamiek, de tijd tussen het indrukken van de toetsen en de pauze die tussen woorden wordt gelaten. Dit is mogelijk door een sensorsysteem dat in het toetsenbord wordt geplaatst (Van den Boogaerde, 2006).

2.4.2.2 Voor- en nadelen klavierscan

Het voordeel van deze techniek is de goedkope kostprijs. Er dient enkel een softwarepakket te worden geïnstalleerd. Tevens is het een niet-invasieve techniek (niet erg ingrijpend op de privacy). Deze techniek kan, in tegenstelling tot de meeste biometrische technieken, wel gewijzigd worden na grootschalige hacking (BiometricNews, N.d).

Nadelig aan de toetsenbordherkenning is dat het een stressgevoelige techniek betreft. Het typpatroon kan veranderen bij een hogere aanwezigheid van stress of vermoeidheid. Tevens evolueert deze techniek in het leven. De snelheid en de sterkte van indrukken zijn aspecten die veranderen doorheen de levensloop. Verder kunnen concentratiestoornissen het typen beïnvloeden. Een afleiding kan zorgen voor verstrooidheid en bijgevolg het typpatroon aanpassen. Kortom, het is een techniek die heel gevoelig is voor omgevingsstimuli en bijgevolg weinig consistent is.

2.4.3 Handtekeninganalyse

2.4.3.1 Werking

De handtekeninganalyse wordt als een vorm van biometrie beschouwd. Door middel van een speciale pen aan een tablet wordt dit verbonden met een computer voor verdere verwerking en verificatie. De uitgeoefende druk van de pen wordt geanalyseerd, evenals de snelheid, de grootte en de verschillende richtingen van de handtekening (Chaudhari, Pawar & Deore, 2013). Bij een gewone handtekeninganalyse wordt de handtekening geanalyseerd en vergeleken, terwijl bij de biometrische handtekeninganalyse het hele proces van handtekenen wordt bestudeerd. Het is dus een meer dynamische handtekeningherkenning (BiometricNews, N.d.).

2.4.3.2 Voor- en nadelen handtekeninganalyse

In tegenstelling tot de gewone handtekening kan de biometrische handtekening moeilijk worden nagemaakt. Het proces van het handtekenen leent zich immers minder gemakkelijk tot namaak. Hierdoor is het eerder aangewezen om de biometrische handtekening te gebruiken bij belangrijke transacties (BiometricNews, N.d). De techniek is ook niet invasief. Na een grootschalige hacking is het mogelijk om de biometrische gegevens te veranderen. Dit kan bijvoorbeeld niet bij een vingerafdruk. Eenmaal de vingerafdruk is opgeslagen blijft deze voor altijd dezelfde, terwijl (het gedrag van) iemands handtekening gewijzigd kan worden.

Een belangrijk nadeel is dat er enorm veel variatie in handtekeningen bestaat en dat handtekeningen zelden tweemaal identiek zijn. De handtekeningherkenning is tot slot geen stabiele techniek en wordt beïnvloed door ziektes, verouderingsprocessen en medicatie (BiometricNews, N.d).

Naast de hierboven aangehaalde vormen van biometrie bestaan er nog heel wat andere technieken. Biometrie gaat over de lichaamseigen kenmerken van een individu, waardoor de toepassing heel ruim is. Technieken zoals het warmtepatroon van het gezicht, de oorprint, DNA of de manier waarop iemand loopt zijn eveneens mogelijke biometrische kenmerken. In onderstaande tabel worden een aantal fysiologische en gedragsmatige biometrische kenmerken weergegeven.

3 In welke sectoren wordt biometrie gebruikt?

De **financiële sector** is één van de hoofdgebruikers van biometrische gegevens. Dit wordt verklaard door een verhoogde drang naar efficiëntie alsook naar beveiliging. Vanuit de financiële sector werden verschillende projecten opgestart waarbij gebruik werd gemaakt van biometrische gegevens, bijvoorbeeld door Mastercard. Chiptechnologie wordt daarbij gecombineerd met de vingerafdruk. De eerste proeven liepen in Zuid-Afrika en pilootprojecten werden opgezet in Nederland. Na deze testing werd het gebruik van biometrische gegevens ook doorgevoerd in België (De financiële begrippenlijst, 2019). De banken zijn de grootste vragende partij en krijgen het meeste vertrouwen van de burger om hun biometrische gegevens te gebruiken (Febelfin, 2016).

Zowel in Azië als Zuid-Amerika gebruiken banken biometrische gegevens om een extra controle door te voeren. Zo zijn de bankautomaten in Azië en Zuid-Amerika uitgerust met handpalmscanners (Aussems, 2018). De Hongkong and Shanghai Banking Corporation en Barclays bank gebruiken stemherkenning als verificatie van de identiteit.

Ook in het Verenigd Koninkrijk is er een stijgend gebruik van biometrische gegevens in de banksector. Het toenemend gebruik van biometrie kwam er voornamelijk door de stijging van 135 miljoen pond aan fraude in 2010 naar 309 miljoen pond in 2016 (Houses Of Parliament, 2018).

Naast de financiële sector spelen biometrische gegevens een belangrijke rol binnen het **domein van de migratie**. Bovenaan werd reeds een aantal systemen besproken die werden ontwikkeld op nationaal en Europees niveau waarbij biometrische gegevens verzameld worden, zoals AFIS. Handpalmscanners en vingerafdrukken zijn populair bij luchthavens en grenscontroles. De irisscan werd geïmplementeerd in Schiphol in 2001. Niet iedereen was blij met deze maatregel, wat leidde tot een prijsstijging van de jaarabonnementen van Schiphol. Een jaarabonnement werd 10 euro duurder en de prijs van een Privium Plus kaart steeg met 40 euro per jaar (N.d., 2008). Het gebruik van de irisscan werd niettemin positief geëvalueerd: de techniek was tijdbesparend en veel veiliger in vergelijking met de traditionele paspoortcontrole.

In 2002 gebruikte het Bureau van Hoge Commissarissen voor Vluchtelingen in Chicago de irisscan voor het terugsturen van vluchtelingen uit Afghanistan. Na de val van de Taliban werden hulppakketten uitgedeeld aan Afghaanse vluchtelingen die konden terugkeren. De irisscan werd gebruikt om te vermijden dat personen tweemaal een pakket zouden ontvangen of er één ontvangen zonder dat ze hier recht op hadden.

In 2011 werd één van de grootste installaties van gezichtsherkenning in de luchthavens van Panama geplaatst, in de strijd tegen drugssmokkel en georganiseerde criminaliteit. Ook in de Britse luchthavens wordt recent geëxperimenteerd met gezichtsherkenning als self-service boarding. Het manueel controleren van de vliegtuigtickets in de luchthavens wordt hierdoor vermeden (Miranda, 2018). Sinds 2006 bevatten alle paspoorten in het Verenigd Koninkrijk een elektronische chip met daaraan gekoppeld een afbeelding van de eigenaar van het paspoort. De foto's van de reizigers worden vergeleken met de afbeelding op de chip.

De irisscan wordt vaak gebruikt in de **industriële sector**, met name bij toegangscontrole van kerncentrales.

Evengoed stijgt het belang van biometrische technieken binnen de **militaire sector**. Zo speelt anonimiteit een grote rol in het leger. Daarnaast kunnen sneller verbanden worden gelegd tussen personen en incidenten, personen en wapens of personen en aangetroffen goederen aan de hand van biometrie. Dit zou de veiligheid voor de eigen troepen verbeteren en het veiligheidsgevoel van de lokale bevolking vergroten (Van Kleef, 2018).

Allerhande **overheids- en gezondheidsdiensten** tonen interesse in biometrie. Zo gebruikt men in Afrika een biometrische ID-kaart om toegang te krijgen tot overheids- en gezondheidsdiensten. Op deze manier wil men identiteitsfraude bestrijden en de zorg en diensten verlenen aan personen die het echt nodig hebben (Gemalto, 2019).

Wat betreft wetshandhavingsinstanties, maakt de Belgische **politie** gebruik van DNA-gegevens en vingerafdrukken. Hierbij wordt in België de verwerking van DNA-gegevens onder de bevoegdheid van justitie geplaatst, en meer specifiek het Nationaal Instituut voor Criminalistiek en Criminologie (NICC). De verwerking van vingerafdrukken daarentegen behoort tot de politionele bevoegdheid, meer specifiek de Biometric Identification Service (BIS). In 2019 experimenteerde de Federale Politie met gezichtsherkenning op de luchthaven. Het Controleorgaan op de Politionele Informatie gaf aan dat er een aantal wettelijke bezwaren waren waardoor het project werd stopgezet (VRT, 2019).

Sedert 2006 steeg het gebruik van stemherkenning in politie- en inlichtingendiensten om terroristenleiders en drugshandelaars te identificeren. Tot slot worden in het huidige Britse leger zowel vingerafdrukken als irisherkenning gebruikt voor de toegang tot bepaalde basissen (Houses of Parliament, 2018).

Binnen de **forensische wetenschappen** is het gebruik van biometrische gegevens een centraal gegeven. In 2004 werd in Nigeria voor het eerst massaal gebruik gemaakt van vingerafdrukken naar aanleiding van een tsunami, als hulpmiddel ter identificatie van de slachtoffers. Sindsdien worden in Nigeria vingerafdrukken op het rijbewijs geplaatst (Leenders, 2008). Het bekend beeld uit filmscenario's waarbij optische, chemische en fysische methodes worden gehanteerd om sporen van de vingerafdruk zichtbaar te maken en zo de mogelijke dader(s) te identificeren is in de samenleving dagelijkse realiteit (Nationaal forensisch onderzoeksbureau, 2019). Binnen de forensische wetenschap is gezichtsherkenning een veelgebruikte techniek om bijvoorbeeld verdachten of lijken te identificeren. Zo werd Osama Bin Laden geïdentificeerd aan de hand van gezichtsherkenning (Dhairya, 2018).

Het gebruik van biometrische gegevens stijgt tevens binnen de **commerciële sector**. Zo is Apple bijvoorbeeld één van de eersten die de vingerafdruk en gezichtsherkenning als ontgrendeling van een smartphone lanceerden. Recent verklaarde Apple dat ze deze technieken ook wil gebruiken voor het ontgrendelen van de auto, een techniek die de Koreaanse autobouwer Hyundai reeds in 2018 lanceerde. Ook Mercedes en Volkswagen hechten belang aan het gebruik van biometrische gegevens (Digital trends, 2019). Daarnaast werd de irisscan toegevoegd aan de laatste smartphone van Samsung. De implementatie van stemherkenning is evenzeer een feit, door de Google 'voice search' applicatie voor iPhones (Kikel, 2019) en in 2011 werd Siri geïnstalleerd op de iPhone 4S (Assens, 2019).

Sinds 2017 wordt gezichtsherkenning gebruikt in de retailsector, in de strijd tegen het identificeren van potentiële dieven. Gezichtsherkenning wordt niet alleen gebruikt vanuit een veiligheidsoptiek maar eveneens als betaalmiddel (N.d., 2017). In een vestiging van Kentucky Fried Chicken (KFC) in het Chinese Huangzhou is er sinds 2017 een pilootproject 'smile to pay' waarbij klanten betalen door te glimlachen (iStock, 2017).

Er worden bovendien systemen getest waarbij camera's de emoties van klanten detecteren: als een klant ongelukkig is, wordt dit herkend door het systeem en wordt de klant bij het naar buiten gaan aangesproken om de oorzaak te achterhalen van deze emotie.

In België overweegt de winkelketen Carrefour het aanbieden van een betalingssysteem 'My finger' door middel van het geven van vingerafdrukken. Carrefour wil voornamelijk de snelheid en het gebruiksgemak verbeteren. De GBA stelt zich hier echter vragen bij omdat dit systeem een opslag vereist van vingerafdrukken en deze linkt aan de bankkaart van de klant. GBA trekt de noodzaak van deze maatregel niet alleen in twijfel maar ook de proportionaliteit: "*Is je vinger scannen het minst ingrijpende betalingssysteem?"* (Het Nieuwsblad, 2019).

Sociale media maakt evenzeer gebruik van biometrische technieken. In 2010 was er een doorbraak in het gebruik van gezichtsherkenning op sociale media, mede dankzij Facebook. Facebook liet toe om automatisch gezichten te herkennen, waarbij men personen kan 'taggen'. Het automatisch taggen op facebook verdween inmiddels en werd vervangen door een waarschuwing die men krijgt als iemand een foto publiceert waarop men staat. Men kan dan zelf kiezen om zichzelf te taggen, ongetagd te bijven of de foto te rapporteren om deze te verwijderen (Datanews, 2020).

Er moet een verschil worden gemaakt tussen bijvoorbeeld het toepassen van biometrie op klanten, zoals in bovenstaande voorbeelden, of het aanwenden van biometrische gegevens bij personeelsleden. Schoenwinkel Manfield wou op een efficiëntere manier het kassasysteem beheren en werken met een vingerscan van de werknemers alvorens hen toegang te geven tot de kassa. De rechtbank van Amsterdam gaf echter aan dat werknemers niet verplicht kunnen worden om een vingerafdruk af te staan. Dit is in strijd met de Algemene Verordening Gegevensbescherming (AVG). De schoenenzaak had via een gezamenlijk verzoek bij de rechtbank gevraagd naar duidelijkheid of een medewerker mag weigeren de vingerafdruk af te staan voor een nieuw ingevoerd systeem van vingerscanautorisatie. Dit systeem werd door Manfield bovendien aan een tijdsregistratiesysteem gekoppeld. Net dit leidde ertoe dat de kantonrechter aangaf dat er sprake is van verwerking van persoonsgegevens wat volgens de AVG niet toegestaan is (Beveiligingsnieuws, 2019).

Het gebruik van biometrische gegevens wordt ook populairder in **onderwijsinstellingen.** Zo verscheen in 2013 een artikel in Het Laatste Nieuws waarin gesteld werd dat tientallen scholen de vingerafdrukken van hun leerlingen registreren. In Luik werd een systeem met vingerafdrukken geïmplementeerd om zo het hoge aantal spijbelaars terug te dringen en de ongewenste gasten buiten te houden. Ook in Gent, Brussel, Mechelen en Opwijk experimenteren scholen met het gebruik van biometrische gegevens. Het gebruik van biometrische gegevens in onderwijsinstellingen is niet enkel gelinkt aan toegangscontrole maar kan ook betalingen efficiënter laten verlopen. Zo vatte het schooljaar 2018-2019 in de Gentse Sint-Bavohumaniora aan met de

idee om via het scannen van de handpalmen broodjes of fotokopies te betalen (VRT, 2019). De school wil af van de verloren en/of vergeten badges, maaltijdkaarten en cash geld… en werkte een systeem uit waarbij leerlingen hun handpalm laten scannen – GDPR-proof – en op deze wijze eenvoudige betalingen via de handpalm kunnen doen. Dit project werd uitgesteld om een advies te vragen bij de GBA.

Naast de handpalmscan als betalingsmiddel en de vingerafdrukken als registratiesysteem wordt in een Zweedse school een gezichtsherkenningstechnologie gebruikt om de aanwezigheid van leerlingen vast te stellen (Beveiligingsnieuws, 2019).

Samenvattend kan gesteld worden dat het gebruik van biometrie zich vaak situeert in sectoren waar de beveiligingseisen hoog zijn. In sectoren zoals de bouw, farmacie en media is het gebruik van biometrie minder uitgesproken. Ook in de gezondheidssector is dit minder ingeburgerd. Een mogelijke verklaring hiervoor is het belang aan hygiëne binnen deze sector waarbij technieken zoals de vingerafdruk en handpalmafdruk de hygiëne in gedrang brengen (Van Eeckhout & de Beelde, 2003).

Global Market Insights (2017) maakte een voorspelling van de sectoren waarin biometrie zou aangewend worden tussen 2017 en 2024. Op basis van een aantal uniek ontwikkelde modellen probeert men de marktevolutie in te schatten en te voorspellen. "*The models are econometric or technical, based on the time period under consideration and are iterative and customizable in nature so as to minimize errors and improve accuracy*". Parameters die aanwezig zijn in hun model zijn drivers van groei, knelpunten en keytrends, dynamieken in toepassingsmarkten, regelmatige en politieke updates en hun impact, trends en ontwikkelingen van technologie, ruwe demand & supply dynamieken en handelsstatistieken. Op basis van interviews met belangrijke bedrijfsleiders, experten en potentiële klanten werden inzichten verzameld in hoe de biometrie zal evolueren.

Global Market Insights beschrijft de cijfers van 2016 waarin USD 12.03 Billion wordt uitgegeven aan de biometrische industrie. Biometrie wordt in de volgende sectoren in hoofdzaak toegepast:

Application Trend (2016) - Biometrics Global Market Report	
Government	23,05%
Defense Services	14,33%
Banking and Finance	5,90%
Consumer Electronics	12,48%
Healthcare	12,61%
Transport/Visa/Logistics	27,47%
Others	4,15%

Tabel 1: Application trend (2016). Source: Global Market Insights (2017)

Als dit bekeken wordt per regio, dan vinden we de volgende regionale trend terug in 2016:

Regional Trend (2016) - Biometrics Global Market Report	
North America	33,13%
Europe	27,23%
Asia Pacific	25,39%
Latin America	9,15%
MEA (Middle East and African regions)	5,10%

Tabel 2: Regional trend (2016) - Source: Global Market Insights (2017)

Biometrische systemen zullen een blijvende groei kennen omwille van verschillende redenen, aldus Global Market Insights: irisherkenning (een toenemend gebruik ervan in smartphones) en stemherkenning zullen toenemen omwille van de eenvoudige toegankelijkheid en flexibiliteit wat resulteert in een hogere productiviteit.

De technologische innovaties en de stijgende mobiliteit creëren een nieuw domein voor de bank- en financiële sector. "*The biometrics market will have a tangible effect on the future of transport and logistics applications, providing vehicle safety and tracking systems. Each vehicle driver has a unique biometric information that*

provides safety and necessary information to the management for enhanced decision making and individual performance evaluations". De toepassing van biometrie in de transportsector zal sterk groeien om volgende voordelen na te streven: identificeren van anomalieën, waarschuwing van excessief brandstofverbruik, detectie van niet geautoriseerd gebruik van een voertuig en de reductie van onkosten voor overuren.

Er wordt voorspeld dat Azië-Pacific voornamelijk een sterke groei inzake biometrie zal kennen door de groeiende vraag naar veiligheid in landen van deze regio. Stijgende investeringen in slimme veiligheidsoplossingen door regionale overheden om de vitale infrastructuren te beschermen zoals luchthavens, banken, defensie faciliteiten en stock wissels dragen bij tot een groeiende industrie. Ook het groeiende aandeel e-paspoorten en verscheidene nationale identificatieprogramma's, zoals het Aadhaar project by Unique Identification Authority of India (UIDAI) zullen een stimuli zijn voor een groeiend marktaandeel van biometrie. "*Products, such as automated and non-automated fingerprint identification systems, facial recognition systems across various government facilities, banks, enterprises and security establishments, are anticipated to boost the biometrics market growth*".

Het stijgend gebruik van biometrie in verschillende mobile devices, gezondheidszorg en financiële instituties had een positieve impact op de groei van de biometriemarkt. Er is bovendien een constante technologische vooruitgang. Dit blijkt onder andere uit mobile banking die een hoge acceptatie kreeg van de gebruiker door zijn veiligheidsfunctie. Dit heeft de groei alleen maar aangewakkerd. Ook het aanwenden van de biometrie in criminele identificatie gepaard gaande met overheidsinitiatieven die gebruik maken van biometrie waren een stimulans voor de industriële groei.

Er worden in het Global Market Insights report (2017) een aantal sterktes opgesomd opdat de industrie van biometrie zou blijven groeien. Dit zijn: "*rising security concerns, strong demand from goverment sector in North America, Compulsion of e-visas and e-passports for new applicants in North America, rapid technological advancements in Europe, wilde usage in military & IT in Europe, favorable regulatory scenario in APAC, increasing goverment expenditure on security enhancement in LATAM, increasing deployment of face recognition scanners in LATAM, modernizes identification process for voter equality in MEA, mandatory government regulations in MEA*". Er zijn ook een aantal industriële valkuilen zoals: "*high capital investment, stored data security concerns, unfeasible deployment at all border exists in North America, Technology related issues in North America, data privacy concerns in Europe, budget constraints in APAC, spoofing attacks in LATAM, system vulnerability in MEA*".

Onder de rising security concerns worden zaken begrepen zoals identiteitsfraude, groeiende terroristische dreigingen, diefstal van kritische informatie of data, … Dit leidt tot de implementatie van biometrie op grote schaal in IT-systemen van de overheid, mobile banking en draagbare device authenticatie. De militaire sector implementeert biometrische technieken aan de grenzen in verschillende landen door de stijgende veiligheidsvraagstukken, wat gerelateerd is aan stijgende terroristische activiteiten. Ook het toenemend aantal telefoonhackings of diefstal van identiteitsdata van mobiele telefoons steeg waardoor gebruikers bezorgd werden. De biometrische technologie kan preventief gebruikt worden om de persoonlijke identiteitsinformatie te beschermen.

Een stijgend aantal incidenten van criminele of frauduleuze aard en activiteiten van terroristen zorgen voor de groei van de aanwending van de irisscan. De veiligheid en de accuraatheid van data door bijvoorbeeld gebruik te maken van een irisscan maakt dergelijke biometrische technieken bijzonder populair. De irisscan wordt beschouwd als één van de meest accurate en betrouwbare identificatiesystemen die gebaseerd worden op de unieke karakteristieken van de iris. De iris zit ook beschermd achter het ooglid waardoor het minimaal beschadigd kan worden.

De biometrische industrie is erg gefragmenteerd. Een stijgend aantal incidenten van criminele en terroristische daden zorgt er ook voor dat de marktspelers geavanceerde technologische oplossingen aanbieden om de veiligheid te garanderen. Door de gevoeligheid en vertrouwelijkheid van data van biometrische technieken – zoals vingerafdrukken, stem, gezicht, … dient het beschermd te worden tegen eender welke vorm van misbruik.

Ook facial recognition zal blijven stijgen, aldus het Global Market Insights report, en dit heeft te maken met een lage mate van indringendheid en een erg hoge accuraatheid. Facial recognition is in staat om op een zeer eenvoudige manier een gezicht te herkennen als het gezicht reeds opgenomen staat in de databank.

Als we kijken in welke sectoren de groei van biometrie voorspeld wordt dan zien we de volgende sectoren op de voorgrond treden: overheidssector; Transport/Visa/logistics; Healthcare; Defense Services; Banking and finance (Global Market Insights, 2017).

4 Beknopt juridisch kader en kritische reflecties

4.1 Juridisch kader

Op internationaal niveau is een belangrijk wetgevend kader inzake biometrie de General Data Protection Regulation (GDPR) of Algemene Gegevensverordening (AVG). Deze Europese verordening is rechtstreeks van toepassing in alle landen van de Europese Unie en gaat over de verwerking van persoonsgegevens. Deze verordening is eveneens van toepassing op de landen buiten de EU die gegevens verwerken van inwoners van de lidstaten (D'huys & Witsenburg, 2018).

In België bestaat sinds 1922 de privacywet dus de GDPR is geen nieuw gegeven. Het grote verschil is dat er vóór de GDPR geen duidelijke sancties voor overtredingen omschreven werden. Sinds de invoering van de GDPR is dit echter veranderd en kunnen boetes opgelegd worden. Ook veranderde de privacy commissie sindsdien van naam in de gegevensbeschermingsautoriteit (GBA). Met deze nieuwe naam was het de bedoeling om de uitbreiding van bevoegdheden te benadrukken. Wanneer gesproken wordt over de General Data Protection Regulation, staan twee concepten centraal: de persoonsgegevens en de verwerking ervan.

De persoonsgegevens zijn stukjes informatie over geïdentificeerde of identificeerbare personen. Alledaagse voorbeelden zijn de naam, het adres, de gezinssamenstelling of het opleidingsniveau van de persoon. Er wordt nog een extra categorisering toegevoegd, namelijk de 'bijzondere persoonsgegevens', waar ook biometrische gegevens onder geclassificeerd worden. Hiervoor gelden extra regels. Voorheen werden persoonsgegevens enkel gezien als gevoelig indien ze werden gebruikt om de raciale afkomst of de gezondheidstoestand van de betrokkene te achterhalen (Europees Parlement & De Raad, 2016).

Een tweede concept is de verwerking waarbij het verwerken van gegevens 'het bewerken, al dan niet aan de hand van een geautomatiseerde procedure, met betrekking tot de persoonsgegevens' impliceert. Voorbeelden zijn het verzamelen, bewerken, verspreiden, ter beschikking stellen of wissen van de gegevens (Europees Parlement & De Raad, 2016).

Voor de verwerking van deze gegevens worden verschillende vereisten uiteengezet. Ten eerste moeten de gegevens worden verwerkt op een wijze die ten aanzien van het betrokken individu rechtmatig, behoorlijk en transparant is. Ten tweede moeten de gegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen ze vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. Tevens moet het gebruik van de gegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Daarnaast moeten de gegevens juist zijn en zo nodig worden geactualiseerd. Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, snel te wissen of te rectificeren. Ook mogen de gegevens niet langer worden bewaard dan nodig voor de desbetreffende doeleinden. Ten slotte moeten passende technische en organisatorische maatregelen worden genomen om de beveiliging van de gegevens te waarborgen, zodat de gegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging[2].

Belangrijk is dat in artikel 9 van de General Data Protection Regulation staat dat de verwerking van gevoelige persoonsgegevens waaruit ras of etnische afkomst afgeleid kan worden en de verwerking van genetische of biometrische gegevens met het oog op unieke identificatie van een persoon verboden is. Er kan enkel van dit verbod worden afgeweken indien de betrokkene toestemming geeft, indien het van algemeen of wetenschappelijk belang is, indien het noodzakelijk is voor historische of statistische doeleinden.... Dit verbod is niet van toepassing in kader van de preventie van criminaliteit door de LEA's (Law Enforcement Authorities). Hierbij is wel strikte noodzakelijkheid vereist (Kindt, 2018).

Het is tot slot niet onbelangrijk om de wijziging in de nationale camerawet te vermelden. Sinds mei 2018 is het nieuwe Koninklijk Besluit inzake aangifte van plaatsing van gebruik van bewakingscamera's in werking getreden, samen met de General Data Protection Regulation. De aangifte van bewakingscamera's gebeurt voortaan bij de politiediensten (Federale Overheidsdienst Binnenlandse zaken, 2018).

[2] General Data Protection Regulation. (2018, 25 mei).

Naast de GDPR zijn er andere internationale juridische kaders zoals de bescherming van persoonlijke gegevens[3] (Council of Europe), de uitwisseling van gegevens tussen politieorganisaties (International Criminal Police Organization, n.d.), verzameling en uitwisseling van gegevens van de Europese Unie[4] (2016) en ook de Universele Verklaring voor de rechten van de mens (UVRM) – meer bepaald artikelen 12 en 17 - en het Europees Verdrag tot bescherming van de Rechten van de Mens (EVRM) – zoals artikel 8 - worden in deze context vermeld. Dit betekent dat voor het verwerken van persoonsgegevens rekening moet gehouden worden met verschillende internationale kaders en er een afweging dient gemaakt te worden tussen het algemeen belang of het belang van de verantwoordelijke tegenover het recht op bescherming van het privéleven (De Beuckelaere, 2018).

Binnen de GDPR werd voor de verschillende lidstaten ruimte gelaten om eigen accenten te leggen en specifieke voorschriften te voorzien. In september 2018 trad dan ook de Belgische Gegevensbeschermingswet in werking[5]. Één van de krachtlijnen is dat de verwerking van biometrische gegevens verboden is, tenzij vrije toestemming wordt gegeven. In artikel 22 van de Grondwet wordt eveneens de privacy van de burger gewaarborgd. In de Grondwet staat dat "*ieder recht heeft op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald*". Tot slot wordt binnen de juridische context ook vaak gerefereerd naar de gewijzigde camerawet van 25 mei 2018.

4.2 Kritische reflecties over het toenemend gebruik van biometrie

Een eerste belangrijke kritische reflectie heeft betrekking op het privacy-concept. Budak, Rajh & Rechner (2017) merken op dat het concept van privacy sterk wordt beïnvloed door culturele aspecten. Privacy is een vaak bediscussieerde term en de betekenis van het begrip privacy is sterk gerelateerd aan de wettelijke, sociale en culturele context van de privacy. "*Different cultures have different approaches to privacy*", schreef Dixon (Budak, Rajh & Rechner, 2017). Deze reflectie is fundamenteel, niet alleen bij navolgende kritische reflecties maar evenzeer in het volgende hoofdstuk, waarin de opinie van de burger wordt bevraagd.

Op nationaal niveau werd vrij recent het wetsontwerp goedgekeurd om digitale vingerafdrukken toe te voegen aan de elektronische identiteitskaart. Dit wetsonderwerp stuitte op behoorlijk wat kritiek. Deze goedkeuring werd gegeven ongeacht het negatief advies van de GegevensBeschermingsAutoriteit (GBA) over dit wetsvoorstel. Een andere kritische stem kwam er vanuit wetenschappelijke hoek. Een studie van de KU Leuven stelde dat deze maatregel onduidelijk, disproportioneel en bijgevolg bijzonder risicovol is. Het gebruik van biometrische gegevens en de potentiële gevolgen van hacking zouden niet in verband staan met het doel en de effectiviteit ervan, namelijk de bestrijding van identiteitsfraude. Volgens professor Preneel kan identiteitsfraude worden bestreden met de bestaande gegevens op de identiteitskaart, zoals de foto. Daarenboven wordt de methode van de opslag van biometrische gegevens op de identiteitskaart in vraag gesteld. De bedoeling is om de vingerafdruk te bewaren op een contactloze chip, maar deze zouden heel eenvoudig te inactiveren zijn door bijvoorbeeld de identiteitskaart kort in de microgolfoven te plaatsen. Op deze manier kunnen de vingerafdrukken niet meer worden achterhaald (Belga, 2019). Ten slotte is het de bedoeling om deze vingerafdrukken op te slaan in een centrale databank. Professor Preneel geeft aan dat een hacking bijgevolg impact kan hebben op de rest van iemands leven.

Ook Matthias Dobbelaere-Welvaert, een fervent voorvechter van het recht op privacy, ondersteunde deze studie en richtte de 'Stopvinger-beweging' op, via het sociale mediakanaal Twitter. Binnen deze beweging wordt onderzoek gedaan naar de juridische en technische gevaren van dit wetsvoorstel, waarmee Dobbelaere-Welvaert aankaart dat dit voorstel in strijd is met het eerder vermelde artikel 22 van de Grondwet (Dobbelaere-Welvaert, 2019).

Matthias Dobbelaere-Welvaert is een tegenstander van de verplichte vingerafdruk op de ID-kaart. Hij ging samen met een aantal gelijkgezinden en advocaat Geert Lenssens naar het Grondwettelijk Hof om deze wet ongedaan te maken. Zij stellen dat de drijfveer voor het opslaan van de vingerafdruk, namelijk het bestrijden van identiteitsfraude, een illusie is. Het grootste deel van identiteitsfraude wordt op het internet gepleegd zonder een elektronische ID-kaart. Eveneens halen zij aan dat de wet indruist tegen het proportionaliteitsbeginsel en de General Data Protection Regulation.

[3] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (1985, 1 oktober).
[4] On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. (2016, 26 april).
[5] De Belgische Gegevensbeschermingswet treedt vandaag in werking. (2018, september)

Er worden enkele artikelen van de General Data Protection Regulation geplaatst ten opzichte van het wetsontwerp. Zo wordt de vraag gesteld in welke mate biometrische toegangscontrole verenigbaar is met het principe van nauwkeurigheid. Biometrische toegangscontrole baseert zich op kansrekening. Er wordt gekeken in welke mate bijvoorbeeld de afgenomen vingerafdruk overeenstemt met de opgeslagen vingerafdruk. Dit levert enkele statistische problematieken op zoals het foutief aanvaarden of verwerpen van de nulhypothese. In de praktijk impliceert dit dat een persoon wordt toegelaten in een gebouw zonder dat dit de effectieve persoon is. Anderzijds is het mogelijk dat iemand niet wordt toegelaten terwijl hij/zij in theorie wel zou toegelaten moeten worden.

Artikel 5 van de GDPR stelt dat de persoonsgegevens voor gerechtvaardigde doeleinden verzameld moeten worden. De vraag wordt gesteld in welke mate dit het geval is bij het 'taggen' van gezichten op foto's op Facebook. Ondanks privacybezwaren heeft Facebook deze functie terug ingevoerd in maart 2018 (Taha, 2018).

De reden waarom biometrische technieken aan een opmars bezig zijn, heeft frequent te maken met de tekortkomingen van andere vormen van toegangscontrole (namaken van paspoorten, verliezen van badges…), een tweede kritische reflectie. Biometrische gegevens kunnen vervalst worden, het zogenaamde biometric spoofing. Tsutomu Matsumoto slaagde er in 2003 in om gummiberen vingers te maken die werden erkend door vingerafdruklezers. Ook de gezichtsherkenning die door Apple werd gebruikt in de iPhone X werd eenvoudig misleid door middel van een foto of een masker vanuit een 3D-printer. Eveneens werd in 2012 aangetoond dat het mogelijk is om replica's van de irissen te maken (Redactie, 2018). Het bewaren van biometrische gegevens is bovendien niet zonder risico's. Zo werd in 2015 bij het OPM (Office of Personnel Management, het federaal bureau dat alle gegevens van de ambtenaren bijhoudt in de VS) een database met 5,4 miljoen vingerafdrukken gestolen (Sustronck, 2019). Het bijhouden van data en de mogelijkheid dat datasets worden gestolen is één van de grootste zorgen bij critici.

Meer en meer wordt gebruik gemaakt van biometrische gegevens in scholen. De vraag wordt door critici geopperd of dit wenselijk is, een derde kritische reflectie. Men creëert op deze wijze van jongs af aan het idee dat kinderen opgroeien in een omgeving van wantrouwen en permanente controle, waarin een doorgedreven toezicht als vanzelfsprekend wordt beschouwd. Daarnaast worden kinderen niet bewust gemaakt om zorg te dragen voor documenten zoals een studentenkaart, en worden bijgevolg een aantal leerkansen ontnomen. Door een biometrische toegangscontrole wordt de menselijke interactie tot een minimum herleid (De Geest, 2013).

Heel wat biometrische technieken worden gebruikt in het dagelijks leven en er wordt vaak verwezen naar landen zoals China en Japan. Zo gaat de gezichtsherkenning erg ver in China en wordt wel eens het woord 'digitaal totalitarisme' in de mond genomen. Wanneer iemand in China een verkeersovertreding begaat, registreren camera's de verkeersovertreder op basis van gezichtsherkenning en worden vervolgens foto's van de overtreder gepubliceerd op een groot scherm. Op deze manier wordt ingespeeld op de schaamtecultuur die heerst in China en andere Oosterse Landen (Bruggeman, 2018). Biometrische technieken worden ook op een vrij verregaande wijze geïmplementeerd in China waarbij gezichtsherkenning wordt toegepast indien men toiletpapier gebruikt. De bedoeling hiervan is om diefstal van grote hoeveelheden toiletpapier, zoals in het verleden frequent gebeurde, te vermijden (BBC, 2017).

Studies over het gebruik van biometrische gegevens bewezen dat dit kan leiden tot sociale uitsluiting, een laatste reflectie. Zo zijn bepaalde biometrische technieken zoals de irisscan en de gezichtsherkenning moeilijk toepasbaar bij vrouwen met veel make-up of gesluierde vrouwen. Dit kan zorgen voor een minderwaardigheidsgevoel of discriminatie[6].

[6] https://sites.google.com/site/cs181biometrics/ethical-issues

5 Een studie naar de publieke opinie

5.1 Een digitale samenleving = een veilige samenleving?

De implementatie van nieuwe technologieën wordt steeds meer als noodzakelijk beschouwd om zich te beveiligen tegen toenemende risico's. Dergelijke technologieën worden vaak geïmplementeerd zonder dat de burger hierover wordt bevraagd. Er wordt verondersteld dat de burger veiligheid cruciaal vindt – en bereid is om zijn privacy hiertoe in te ruilen - waarin het centrale gedachtegoed speelt van: "*als men niets verkeerd doet, als men niets te verbergen heeft…*", men geen probleem heeft om zijn privacy op te geven. Deze manier van denken laat toe om een grotere overheidscontrole mogelijk te maken door surveillantie, wat zorgt voor een hogere veiligheid. Maar wat denkt de burger over de aanwending van digitale technieken? In hoeverre is er een acceptatie en hoe groot is deze acceptatie? Bij het bestuderen van deze opinie spelen enkele factoren een rol zoals het vertrouwen in overheden in het managen van die technologieën, technologie-optimisme, de perceptie van risico's en bedreigingen, demografische factoren en sociaal-politieke attitudes…

5.2 Factoren die de publieke opinie beïnvloeden

In 2015 vond een grootschalig Europees onderzoek plaats, SurPRISE waarin gepeild werd naar de mate van aanvaardbaarheid van sensortoepassing door de burger. De perceptie van de bevolking ten aanzien van dergelijke toepassingen werd bestudeerd in negen Europese landen (Pavone, Santiago & Degli-Esposti, 2015)[7]. Door middel van een literatuurstudie onderscheidden Pavone et al. (2015) 30 factoren die de burgers perceptie over sensortechnologieën (cfr. Surveillantie) beïnvloeden. Op basis van kwalitatief onderzoek onderscheidden zij zeven factoren die een significante invloed hebben op hoe burgers denken over de sensortechnologie:

- Algemene houding ten aanzien van de technologie;
- Betrouwbaarheid van instituties;
- Sociale 'nabijheid' (het richten van technologieën op specifieke groepen zoals verdachten);
- Gevoel van inbreuk;
- Waargenomen effectiviteit;
- Substantiële privacy zorgen en;
- Leeftijd.

Factoren zoals 'gevoelens van veiligheidsdreiging', 'de mate van vertrouwdheid met de sensortechnologieën', 'inkomen', 'opleiding', de 'fysieke nabijheid van de technologie', 'de verwachting dat de technologie in de toekomst van grote invloed zou zijn' en de 'voorstelling dat veiligheid en privacy een uitruil zijn' zijn van weinig of indirecte invloed op de publieke acceptatie van de sensortechnologieën.

Rathenau Instituut bracht in Nederland evenzeer deze factoren in kaart (Biesiot, de Bakker, Jacquemard & van Est, 2018). De navolgende tabel bevat alle factoren waarop de toepassing van sensortechnologie wordt beoordeeld ter verhoging van de veiligheid en de leefbaarheid door burgers.

Burger (subject)		**Sensortoepassing (object)**	
Persoonskenmerken		**Sensortechnologie**	
	Geslacht		type sensor(data)
	Leeftijd		Invasiviteit (gevoel van inbreuk, mate van persoonlijke informatie)
	Inkomen		Privacy-by-design ontwerp
	Opleiding		
Houdingen		**Sociale praktijk en actoren**	
	Openstaan voor delen van informatie		Uitvoerder (publiek/privaat)

[7] Infra

	Vertrouwen met sensortechnologie		Doel en proportionaliteit
	Algemene houding jegens technologie		Combinatie van technische en sociale middelen
	Substantiële privacy zorgen		Effectiviteit
	Gevoelens van veiligheidsdreiging		Instemmingsmogelijkheid (opt-in approach)
	Veiligheid en privacy als uitruil		Transparantie over doel en omgang met sensordata, incl. gegevensbescherming, aansprakelijkheid en toegang tot data
			Privacy-by-design praktijken (gerichte dataverzameling)
Directe sociale omgeving		**Maatschappelijke, institutionele context**	
	Vertrouwen in (wijk)agenten en beveiligers		Vertrouwen in instituties
			Regulering en toezicht daarop

Tabel 3: Factoren die invloed hebben op perceptie over sensing (Bron: Rathenau Instituut)

In België zoomen Vermeersch, Vandenbogaerde en De Pauw (2018) dieper in op specifieke gebeurtenissen, zoals *external shocks or threats*. Zo kan een terrorismeaanslag de houding van de burgers beïnvloeden en ervoor zorgen dat bepaalde technologieën sneller worden aanvaard. Het is echter niet evident om dergelijke gebeurtenissen te voorspellen en de impact hiervan op de publieke opinie te meten. Dit gebeurt door experimentele studies waarin de effecten van een externe shock worden gesimuleerd. Vermeersch et al. (2018) onderzochten het effect van reële shocken naar aanleiding van de terrorismeaanslagen van 2015. Zij gaan na of 1) de respondenten bereid zijn om hun privacy in te ruilen voor gouvernementele controle en 2) of zich dit vertaalt in een grotere acceptatie van vier specifieke technologieën die kunnen gebruikt worden in de strijd tegen criminaliteit zoals "*smart CCTV, behavioural profiling, radio frequency identification (RFID) and DNA-databases*" (Vermeersch, Vandenbogaerde & De Pauw, 2018). Deze opgesomde technologieën worden meermaals beschouwd als zijnde de maatregelen tegen terrorisme. Verder werd gekeken of de aanslagen van Parijs de opinie van studenten veranderde op de volgende domeinen: vertrouwen in overheden, risicoperceptie, angst voor criminaliteit, attitude over *privacy-control trade off* en gebruik van *surveillance oriented security technologies* (SOST's). Er werd eveneens onderzocht of de verandering in attitude afhankelijk is van de angst als een persoonlijkheidsvariabele.

Vermeersch et al. (2018) vergeleken onderzoeksgegevens uit twee panels (2014 en 2016) en concluderen dat een hogere risicoperceptie leidt tot meer acceptatie van gouvernementele controle: "*respondents perceive higher risks – even risks that are not terror-related – in their direct environment (neighbourhood) and they are more inclined to support governmental control over privacy in the privacy-control trade off in 2016 that they were in 2014".* Er is echter geen verandering in acceptatie van het gebruik van SOST's tussen 2014 en 2016. "*This indicates that, while in general respondents favour more control even if this may affect their privacy compared to the 2014 wave, this does not mean that they are ready to accept concrete measures. This may suggest, in line with increasing evidence thereof, that a privacy-control trade-off is an overly simplified way to interpret public opinion on the acceptance of SOSTs*".

Gopal en Murale (2018) bestuderen bij senioren de acceptatie van technologie. Zij stellen dat "*Acceptance of technology is about a person's intention to use the technology and if he starts and keeps using it happily. It is influenced by many factors, such as, prior experience with technology, self voluntariness of use and*

purchasing power. It is difficult to change those factors. Fortunately, other factors can be influenced more easily." Op basis van Gopal en Murales onderzoek blijkt dat als senioren de gebruiksbarrières van de computer kunnen overkomen, ze meer enthousiast en bereidwillig zijn om deze technologieën te gebruiken.

"*De digitale samenleving is gebaseerd op vertrouwen*", aldus Visser en Hoorweg (2018) waarbij de burger er op vertrouwt dat de overheden en organisaties op een integere manier omgaan met data. Dit impliceert dat de waarheid niet wordt gemanipuleerd en de burger ervan uitgaat dat zijn persoonsgegevens niet te grabbel liggen. Dit vertrouwen kwam echter onder druk te staan door allerhande publieke en private organisaties die er in slagen om data te verzamelen en deze te gebruiken voor discutabele doeleinden. De technologische ontwikkelingen creëren hierdoor veeleer een negatieve in plaats van positieve perceptie. Anderzijds beïnvloedt de inzet van disruptieve technologie de strijd tegen criminaliteit sterk, zonder dat de privacy van de individuen wordt geschaad. Er worden door de politie ook zelf applicaties en websites ontwikkeld opdat een betere opsporing gegarandeerd wordt. Zo is er in Nederland sprake van de zogenaamde Q-teams. Dit leidde onder meer tot het gebruik van gamification in de opsporing, wearables, dashcams en beveiligingscamera's.

"*In hoeverre slimme technologie daadwerkelijk kan bijdragen aan een veilige samenleving?"* is de vraag die Visser & Hoorweg zich stellen. Een tweede centrale vraag is of er een draagvlak is bij de bevolking voor het aanwenden van deze technologie. De vraag "*Hoe staat u tegenover onderstaande middelen om de veiligheid te vergroten?*" wordt ingevuld met middelen zoals bodycams door politie (op borst, schouder of helm), biometrie voor het bepalen van je identiteit, drones, camera's in de publieke ruimte die afwijkend gedrag van (groepen van) mensen analyseren en camera's in de publieke ruimte met gezichtsherkenning. De respondenten worden gevraagd om een antwoord te formuleren op een schaal van zeer positief tot zeer negatief. Dit genereert volgende resultaten:

- Biometrie voor het bepalen van je identiteit: 25% is zeer positief, 31% positief, 31% neutraal, 13% negatief en 5% zeer negatief.
- Camera's in de publieke ruimte die afwijkend gedrag van (groepen van) mensen analyseren: 34% antwoordt zeer positief, 40% positief, 20% neutraal, 4% negatief en 2% zeer negatief.
- Camera's in de publieke ruimte met gezichtsherkenning: 30% antwoordt zeer positief, 34% positief, 24% neutraal, 9% negatief en 4% zeer negatief.

Tot slot gaan we in op de volgende stelling "*Ik heb er vertrouwen in dat de overheid mijn verzamelde gegevens rechtmatig gebruikt, veilig opslaat en zo mijn privacy voldoende beschermt.*" 10% is het 'helemaal eens' met deze stelling, 43% 'mee eens', 28% 'niet mee eens of oneens', 15% 'mee oneens' en 4% 'helemaal mee oneens' (Visser & Hoorweg, 2018). Een gelijkaardige vraag wordt gesteld in de Global Web Index bij Nederlandse internetgebruikers en 50% maakt zich zorgen over het gebruik van persoonlijke data door bedrijven.

Het aanwenden van digitale technologie blijkt steeds een balanceren te zijn tussen hoe de gegevens gebruikt worden opdat men een veiliger samenleving krijgt enerzijds en de vraag hoe men ervoor kan zorgen dat de samenleving zich niet onveilig voelt omdat er persoonlijke gegevens worden gebruikt anderzijds.

5.3 Invloed van framing op de publieke opinie

Het gebruik van nieuwe technologieën wordt gelegitimeerd omdat onze samenleving moet beschermd worden tegen ieder denkbaar risico (Vermeersch & De Pauw, 2017). De tendens om alles te controleren en te limiteren wordt door velen bekritiseerd. Enerzijds waarschuwen verschillende wetenschappers dat de Westerse samenleving in toenemende mate wordt geconfronteerd met een overprotectie, een angstcultuur en de idee dat 'omdat nieuwe technologieën nieuwe vormen van surveillantie toelaten, deze moeten worden geïmplementeerd'. Anderzijds spreekt men van de 'silent erosion of privacy' als resultaat van een toenemend gebruik van nieuwe technologieën door private/publieke organisaties en overheden binnen een grijze zone van wetten.

Het gebruik van technologie wordt niet altijd negatief geconnoteerd; meer en meer duiken stemmen op die het belang onderschrijven van deze nieuwe surveillancevormen, aldus Vermeersch & De Pauw (2017). Omwille van die reden wordt ook meer en meer onderzoek gevoerd naar het draagvlak en de aanvaardbaarheid van deze technologieën.

Het SurPRISE project (Pavone, Santiago & Degli-Esposti, 2015) gaat hier evenzeer op in, net zoals enkele andere FP7 projecten (PRISMS, PACT). Pavone et al. (2015) tonen aan dat wanneer burgers geïnformeerd worden over de aard van de technologieën, ze de surveillance oriented security technologies (SOST's)

belangrijk en noodzakelijk vinden om de publieke veiligheid te waarborgen. "*However, they voice concerns and uncertainties due to a perceived lack of control and information, questions of accountability and fears about abuses of power, function and mission creep*" (Vermeersch & De Pauw, 2017). Doorgaans heeft men weinig kennis wanneer men zich een opinie vormt. De attitude die bij de burger ontstaat is sterk gerelateerd aan de manier waarop deze technologieën worden 'geframed' in het publieke discours. Daarenboven rekent de burger op de informatie die gegeven wordt.

Vermeersch & De Pauw (2017) gaan dieper in op framing. Zij gaan na 1) of de aanvaarding afhangt van het type frame, 2) of bepaalde voorafgaande attitudes (vertrouwen in publieke autoriteiten, privacy zorgen, risicoperceptie en technologie optimisme) die geassocieerd worden met de aanvaarding van technologie, de relatie tussen acceptatie en framing van technologie opvangen. Framing wordt in hun onderzoek geïnterpreteerd als zijnde "*Frames are patterns of selection, emphasis and exclusion that furnish a coherent interpretation and evaluation of events*" (Vermeersch & De Pauw, 2017). Een treffend voorbeeld in de veiligheidscontext betreft het praten over 'een tool in de strijd tegen criminaliteit' in plaats van 'een tool'. Burgers worden als het ware geforceerd om hun mening te geven over iets dat wordt geplaatst tegen een bepaalde achtergrond.

Er werd door Vermeersch & De Pauw (2017) gevraagd naar de mate van acceptatie (op een schaal van 'helemaal niet aanvaardbaar' tot 'totaal aanvaardbaar') van 4 technologieën die aangewend worden door de publieke overheid. De technologieën betreffen 1) Het gebruik van smart CCTV in de publieke ruimte 2) DNA databanken dat genetisch materiaal van alle burgers bevat 3) Het gebruik van Radio Frequency Identification (RFID) en 4) Gedragsprofiling. Deze technologieën worden in deze context gebruikt door publieke overheden.

Hun resultaten tonen dat frames een klein maar consistent effect hebben op de aanvaardbaarheid van het technologiegebruik door de publieke autoriteiten. Dit effect is enkel significant bij gedragsprofiling en voor de volledige aanvaardbaarheidsscore waarbij wordt aangetoond dat de groep die in het security frame zit meer geneigd is om het gebruik van technologie te accepteren dan de groep die blootgesteld wordt aan het privacyframe. Of framing een effect heeft op vooraf bestaande attitudes is niet duidelijk omdat er geen verband wordt gevonden. Respondenten die de publieke autoriteiten vertrouwen, zullen sneller geneigd zijn om het gebruik van technologie door deze autoriteiten te aanvaarden. Echter hoe meer zorgen men zich maakt inzake privacy, hoe minder men geneigd is om het gebruik van deze technologie te aanvaarden. Respondenten die een hoge graad van technologieoptimisme hebben, zullen dit sneller aanvaarden.

Individuen die een hogere risicoperceptie hebben, zijn meer geneigd om deze technologieën te aanvaarden vanuit een security framework dan vanuit een privacyframework. In het privacyframework wordt ook een verband gevonden tussen het vertrouwen dat men heeft in de autoriteiten en de mate van acceptatie terwijl dit vertrouwen in een security framework minder aan de orde is. "*Although framing experiments can only reflect a real public debate in a very simplified way, they may show us how sensitive individuals are for certain arguments. Individuals are sensitive for both arguments, security and privacy, but not always in a way that radically changed their minds*", aldus Vermeersch & De Pauw (2017).

Mitrou, Drogkaris & Leventakis (2018) bestuderen de perceptie van videobewaking in Griekenland. Ze verwijzen naar eerder onderzoek – PACT (Public Perception of Security and Privacy: Assessing Knowledge; Collecting Evidence, Translating Research into Action) - een driejarig project van het Seventh European Framework Programme (2012-2015). In het PACT project wordt door middel van een survey getest of respondenten *security and surveillance technologies* zonder bedreiging voor de privacy prefereren op deze die wel een bedreiging kunnen impliceren. De respondenten geven de voorkeur aan CCTV camera's die data opslaan voor een welbepaalde tijd en toegankelijk zijn voor Law Enforcement Agencies. Ze verkiezen daarnaast CCTV camera's die bijvoorbeeld gebruikt worden voor reisdoeleinden, zoals in stations, en prefereren camera's die gezichten herkennen. Op de tweede plaats komt een systeem dat achtergelaten zakken kan detecteren en op de derde plaats staat een systeem dat verdachte gedragingen en bewegingen van mensen herkent. Een standaard CCTV wordt als vierde voorkeur opgegeven.

In de PRISM surveys, die ingaan op crow surveillantie, staat telkens dat de meest sceptische landen op het vlak van monitoring Griekenland, Australië en Duitsland zijn. Mitrou, Drogkaris & Leventakis (2017) concluderen dat de Griekse opinie sterk wordt beïnvloed door wantrouwen en zorgen omtrent privacy, demografisch en socio-economische karakteristieken zoals leeftijd, geslacht en inkomen. Surveys gingen niet in op de specifieke impact van de Griekse economische crisis, het is echter aannemelijk dat de Griekse crisis een impact heeft op de perceptie van dataprotectie. De surveillantie stijgt onder meer door een toenemende angst voor criminaliteit (eigendomsdelicten, illegale immigratie, politiek geweld, corruptie) en tegelijkertijd blijft het vertrouwen in de overheid erg laag. "*Especially in an environment of economic and social crisis, when uncertainty is rising on multiple levels, the prevention and removal of risks has become a social and political*

expectation. In such a context of 'stage-set-security' the presence of CCTV is a symbol of surveillance and state security but also of 'safety' in a society in which almost everything is seen as a potential source of risk and where insecurity dominates" (Mitrou, Drogkaris & Leventakis, 2017). Er wordt geconcludeerd dat er sprake is van een Griekse paradox waarbij de Grieken zowel veiligheid als privacy cruciaal vinden en deze begrippen elkaar niet noodzakelijkerwijs uitsluiten.

Van den Broek, Ooms, Friedewald, van Lieshout & Rung (2017) bevestigen de resultaten van het SurPRISe project alsook deze van het PRISM project waarin veiligheid en privacy niet noodzakelijk aan elkaar gelinkt zijn en burgers beide willen. Deze relatie wordt bevraagd door vignetten aan respondenten voor te leggen. Een eerste conclusie is dat de attitude ten aanzien van privacy sterk afhangt van de veiligheidscase omdat de graad van acceptatie sterk varieert: "*We conclude that respondents make a distinction between actions that may counter a legitimate interest of EU citizens (gathering for demonstrations as a fundamental right) and actions that are meant to safeguard the majority of EU citizens (and protect them against potential violent behavior with no direct legitimate basis*)", aldus Van den Broek et al. (2017). Een tweede belangrijke conclusie is dat het vertrouwen in instituties van vitaal belang is "*and that trust in public institutions correlates positively with acceptance of privacy intrusive measures".* In derde instantie is het type actor dat de informatie verzamelt belangrijk: over de publieke sectoren is er meer aanvaarding dan private sectoren. Een hoog niveau van 'privacy awareness' beïnvloedt de aanvaardbaarheidsniveau 's op een negatieve manier terwijl een hoog niveau van veiligheidszorg positief correspondeert met het aanvaardbaarheidsniveau.

5.4 Acceptatie van technologie in een slimme stad

De Belgische Smart City Meter van 2018 (Imec, 2018) gaat na hoe burgers het concept van slimme stad en achterliggende technologieën ervaren. Er wordt gepeild naar een aantal aspecten zoals data, data-deling en privacy. Er wordt bovendien ingegaan op hoe burgers een slimme stad percipiëren, wat hun verwachtingen hieromtrent zijn en welke aanbevelingen er zijn voor de overheid, bedrijfswereld en burger. Via een quotasteekproef worden respondenten geselecteerd. Er hebben 2780 respondenten geldig geantwoord.

Op de vraag of de burgers wakker liggen van hun privacy geeft 84% aan dat ze zich wel eens zorgen maken dat hun privacy geschonden wordt.

92% van de respondenten gaat akkoord met de inzet van camera's om de veiligheid van de stad of gemeente te verbeteren. 70% geeft aan zich veiliger te voelen als er veiligheidscamera's op openbare plaatsen of op straat hangen (dit gevoel is iets sterker aanwezig in de stad in vergelijking met de gemeente). De personen die tegen de evolutie van een slimme stad zijn, betreffen ook diegenen die niet akkoord gaan met het gebruik van camera's. Inzake het gebruik van camera's wordt de volgende vraag gesteld: "*In welke mate gaat u akkoord om volgende camera's te gebruiken in functie van de veiligheid?"* **:**

- Gezichtsherkenning in winkelstraten: 56,5% is akkoord, 43,5% is niet akkoord
- Nummerplaatherkenning op invalswegen: 83,9% is akkoord, 17,1% is niet akkoord
- Verkeerscamera type weggebruiker: 84,1% is akkoord, 15,9% is niet akkoord
- Anonieme passantentelling: 79,6% is akkoord, 20,4% is niet akkoord

Op basis van bovenstaande data zien we dat er een verschil is in tolerantieniveau, met andere woorden niet alle camera's worden toegelaten: "*Voor camera's die ook persoonlijke data of kenmerken capteren, zoals gezichtsherkenning, is er bijvoorbeeld minder draagvlak*". Er is een link tussen de bereidheid om data te delen en het accepteren van camera's: "*hoe hoger die bereidheid, hoe hoger de acceptatie*" (Imec, 2018).

5.5 Acceptatie van technologiegebruik door de politie

De Pauw en Vermeersch (2015) bekritiseren dat de inzet van technologie vaak wordt herleid tot een normatief debat. Dit debat wordt gevoerd tussen de zogenaamde "*voorvechters van de veiligheid en de behoeders van de privacy*". De Pauw en Vermeersch (2015) bestuderen de inzet van de technologie vanuit een breder kader, namelijk het surveillantie perspectief. Surveillantie wordt omschreven als de "*doelgerichte, routinematige, systematische en op details gerichte aandacht voor persoonsgegevens met als doel te controleren, te beheersen, te managen of te beschermen*" (De Pauw en Vermeersch, 2015). Surveillantie an sich is niet nieuw maar het gegeven dat heel wat technologische middelen – zoals intelligente geluidscamera's, het gebruik van vingerafdrukken of irisscan als toegangscontrole - kunnen ingezet worden om surveillantie te verwezenlijken wel. De Pauw en Vermeersch gaan op deze wijze aan het normatieve debat voorbij en kijken door middel van

het surveillantie perspectief naar wat de inzet van technologie betekent voor de politie, welke kritische succesfactoren en randvoorwaarden noodzakelijk zijn opdat de politie in 2025 technologie op een goede manier wenst te implementeren. Hun resultaten zijn gebaseerd op een Projectmatig Wetenschappelijk Onderzoek (PWO), uitgevoerd in 2015 aan VIVES hogeschool waarbij onder meer de onderzoeksvraag werd beantwoord: "Wat accepteert de burger aan technologische inzet?". Op basis van hun onderzoek concluderen zij dat de politie niet enkel technologie inzet om de mensen te controleren – een argument dat vaak door de aanhangers van het privacy-perspectief naar voor wordt geschoven – maar voor het communiceren en zichtbaar maken van politiewerk. De politie maakt bovendien doorgaans gebruik van informatie met een publiek karakter.

Rathenau Instituut werd door de politie recent gevraagd om in het kader van het Sensing Programma, de perceptie van de burger te meten en na te gaan hoe burgers aankijken tegen het gebruik van sensing en hoe dit een bijdrage kan leveren aan de veiligheid en leefbaarheid (Biesiot, de Bakker, Jacquemard & van Est, 2018). Digitale sensoren betreffen digitale meetinstrumenten die in staat zijn om allerhande data te verzamelen over zowel de fysieke als sociale omgeving. Binnen de Nationale Politie zijn er heel wat sensoren aanwezig in het politiewerk zoals ANPR en bodycams. Er wordt tevens gestreefd naar het combineren van data uit verschillende bronnen. Cruciaal is dat deze sensoren onderhevig zijn aan evolutie: ze breiden uit (bijvoorbeeld smartphones volgen door wifi-sniffing), ze worden slimmer (facial recognition) en mobieler (sensoren die overal op geplaatst kunnen worden, zoals bodycams). De Nederlandse politie bezit tussen de 500 en 1000 camera's, gemeenten hebben zo'n 3000 camera's op straat en Nederlandse burgers en bedrijven bezitten samen zo'n 1,5 miljoen camera's. Heel wat van deze camera's worden ingezet voor het verhogen van de leefbaarheid en de veiligheid.

Deze sensoren functioneren binnen een nauw 'vernetwerkt data-ecosysteem': "*Er is hierbij sprake van een explosie in het volume van door sensoren gegenereerde data, op deze data worden steeds meer voorspellende analyses toegepast om de enorme hoeveelheden gegevens te verwerken: en dit leidt tot een voortdurende ontwikkeling van verzamel-, opslag en analyse-infrastructuren die zich richten op het inzichtelijk maken van sensordata*". Er wordt in deze context gesproken over de sensorsamenleving en "*De opkomst van deze sensorsamenleving heeft implicaties voor de manier waarop wij gegevens verzamelen en opslaan, maar leidt ook tot nieuwe opvattingen over relaties tussen verschillende groepen mensen (en machines), en noties zoals privacy, macht en toezicht" (Snijders, Biesiot, Munnichs & van Est, 2019).*

De inzet van sensortechnologie moet door de burgers als legitiem worden ervaren, wat de beweegreden is tot dit onderzoek. De politie wil kennis en inzicht verwerven in wat er kan volgens burgers, wat er mogelijk en wenselijk is. Er worden verschillende vormen van toezicht van elkaar onderscheiden. Surveillance betreft het toezicht van bovenaf waarbij autoriteiten burgers en objecten monitoren. Sousveillance betekent dat burgers autoriteiten in de gaten houden terwijl horizontale surveillance betekent dat burgers elkaar bespieden. Zelf-surveillance impliceert dat burgers sensoren inzetten om zich aan de regels van leefbaarheid en veiligheid te houden.

Rathenau instituut wil inzicht verwerven in de factoren die de perceptie van burgers over sensing beïnvloeden. Er wordt hierbij een onderscheid gemaakt tussen de kenmerken van de burger (het subject) zelf (Vindt de burger het acceptabel of niet? Staat de burger open voor het delen van informatie of niet?) en de kenmerken van de sensortoepassing (het object) (Wat voor soort van informatie wordt er verzameld?).

Biesiot et al. (2018) bestudeerden voorafgaand aan deze studie internationale studies waarbij de perceptie van de burger over sensing in kaart werd gebracht. Wat de internationale studies betreft, zien we enerzijds een sterke focus op privacy en anderzijds is er veel Amerikaans onderzoek. Een noemenswaardig grootschalig Europees onderzoek betreft het SurPRISE project (Pavone, Santiago & Degli-Esposti, 2015)[8].

Rathenau instituut onderzoekt de perceptie van de burger door middel van drie sociotechnische scenario's waarin drie eigenschappen van de technologie centraal staan: mobieler, slimmer en uitgebreider. De scenario's richten zich op twee vormen van toezicht: surveillance en horizontale surveillance. Een eerste – mobiele - scenario gaat in op de ontwikkeling van vaste naar mobiele camera's. In het slimme scenario worden slimme sensoren gebruikt zoals automatische gezichts- en gedragsherkenning. Het derde scenario is uitgebreider en impliceert dat allerhande type van data (van verschillende sensoren) samenkomen vanuit een diversiteit aan actoren. Deze scenario's worden voorgelegd aan zes focusgroepen die op een diverse manier worden samengesteld (hoog, laag opleidingsniveau, afkomstig uit een dorp of stad, welgestelde of minder gestelde wijk) en er wordt bovendien een diversiteit nagestreefd inzake leeftijd, geslacht en migratieachtergrond.

[8] Supra.

Nederland wordt door Biesiot et al. (2018) beschreven als een sensorland. "*Sensoren om leefbaarheid en veiligheid te bevorderen zijn digitale technologieën die data verwerken en ook ingrijpen in de fysieke wereld. De zogenaamde 'cybernetische loop' helpt te begrijpen hoe dit werkt*" aldus Biesiot et al. (2018). Er zijn drie cruciale eigenschappen in deze loop: data verzamelen, analyseren en toepassen. De 5 opvallende trends die worden geanalyseerd betreffen:

- "*Er zijn steeds meer politiesensoren en sensordata.*
- *De politie automatiseert een deel van haar kernactiviteiten met slimme sensortechnologie.*
- *Burgers, bedrijven en gemeenten verzamelen steeds meer sensordata.*
- *De politie zoekt nieuwe vormen van samenwerking om de uit de samenleving toekomstige sensordata te gebruiken voor leefbaarheid en veiligheid.*
- *Private partijen gaan zelf speurwerk doen en handhaven met sensordata*".

Hoe meer burgers weten wat er met de informatie gebeurt en kennis hebben over het doel waarvoor de informatie wordt ingezet, hoe meer dit wordt geaccepteerd en er een vertrouwen ontstaat in de politie (Koops & Vedder, 2001; Dinev, Masssimo, Hart, Christian & Vincenzo, 2005).

We zoomen in op de resultaten per scenario. Het eerste mobiele scenario gaat in op het gebruik van camera's (vast of mobiel) door politie. Het feit dat de politie deze beelden gebruikt voor bijvoorbeeld het opsporen van verdachten wordt als positief beschouwd door de deelnemers van de focusgroepen. Er worden echter ook kritische vragen gesteld aangaande de beveiliging en de bewaartermijn van de gegevens, of de mensen moeten instemmen met de opname… Het scenario wordt vervolgens verscherpt waarbij de politie live kijkt naar de camerabeelden. Dit scenario levert verdeelde reacties op waarbij een aantal randvoorwaarden worden geformuleerd: een goede beveiliging van de camera's, een duidelijk doel, effectieve opvolging van de misdaad indien er een misdaad gebeurt… Dit scenario gaat verder waarbij een privaat bewakingsbedrijf de beelden bekijkt in plaats van de politie. Heel wat deelnemers vinden dit een brug te ver: de grootste vrees heeft te maken met het feit dat private bewakingsbedrijven minder gebonden zijn aan regels dan de politie.

Het mobiele scenario maakt vervolgens gebruik van cameratoezicht door middel van bodycams. De deelnemers van de focusgroep stellen dat de bodycam kan gebruikt worden door de politie mits één voorwaarde, namelijk dat de agenten niet zelf kunnen zeggen wanneer ze de bodycam aan- of afzetten. Het scenario wordt omgevormd naar het gebruik van bodycams door veiligheidspersoneel van de Nationale Spoorwegen (NS). Ook hier wordt doorgaans positief gereageerd maar als het veiligheidspersoneel wordt veranderd in pizzakoeriers dan gaan heel weinig deelnemers van de focusgroep akkoord. Burgers die tot slot verdachte of onveilige situaties filmen met hun camera op de smartphone worden aan kritiek onderworpen waarbij men vreest dat burgers het heft in eigen handen gaan nemen.

Het tweede scenario bespreekt de slimme sensoren waarbij software de data van slimme sensoren analyseert zoals automatische gezichtsherkenning. Indien de politie dit gebruikt, worden enkele kritische vragen opgeworpen zoals de bezorgdheid dat men ten onrechte gevolgd wordt, dat er geen toestemming werd gegeven om iets te filmen,… De vraag wordt gesteld of de automatische gezichtsherkenning in de publieke ruimte kan gebruikt worden, wat een negatief antwoord oplevert. Deelnemers formuleren volgende vragen: Wat is verdacht gedrag? Kunnen slimme camera's dit herkennen want bepaalde gedragingen worden misschien ten onrechte als verdacht gekwalificeerd? Op welke plaats gebruikt men dit?

Het derde scenario gaat in op de 'uitgebreide' inzet van sensortechnologie waarbij verschillende types van informatie worden gekruist komende vanuit verschillende sensoren en actoren. Het kassaloze winkelen is hiervan een voorbeeld waarbij velen het gebruiksgemak ervan inzien. Als keerzijde wordt het verloren gaan van het sociale contact opgeworpen. Andere nadelen betreffen het ontstaan van een digitale kloof en het feit dat niet iedereen over digitale vaardigheden beschikt en/of dat dit gepaard kan gaan met een verlies van jobs. Amazon's slimme winkel is het volgende scenario dat wordt uitgerold waarbij alle gedrag dat je stelt in een winkel geregistreerd wordt en bij het verlaten van de winkel wordt het geld afgeschreven van je rekening. De informatie die intussen wordt verzameld, wordt gebruikt om persoonlijke advertenties te versturen.

Het concept van slimme stad wordt voorgelegd aan de focusgroep waarbij steden leefbaar en veilig worden gemaakt door het gebruik van slimme technologieën. Bij de deelnemers van de focusgroep ontstaat opnieuw een dubbel gevoel: aan de ene kant is er het gemak en aan de andere kant heerst er een 'Big brother is watching you'-gevoel. Men is bezorgd dat er door middel van dergelijke technologieën naderhand geen politie meer op straat zal zijn. Er wordt ook kort ingegaan op slimme lantaarnpalen; deze palen meten het geluidsniveau en detecteren bijvoorbeeld een ruzie. De werkbaarheid hiervan wordt in vraag gesteld: 'Werkt dit echt?'.

Tot slot wordt aangegeven dat de inzet van sensoren door burgers altijd verbonden wordt aan de privacy discussie. De idee leeft dat de veiligheidsdoeleinden primeren op privacy. Tijdens de focusgroep is er doorgaans altijd een kantelpunt waarbij bijvoorbeeld een voorstander plots een tegenstander wordt. "*Dit laat zien dat we niet los van praktische en bredere context kunnen spreken over de acceptatie van bepaalde sensoren of technologieën. We kunnen niet stellen dat burgers voor bodycams of tegen wifitrackers zijn; er is bij de inzet van technologie een discussie nodig over het hoe, wat, waar, wanneer en vooral ook waarom*" (Snijders et al. 2019). Deze laatste vragen worden frequenter gesteld bij onbekende technologieën.

5.6 Acceptatie van biometrische technieken

In bovenstaand onderzoek wordt ingegaan op de aanvaarding van technologieën wat zich vaak veruiterlijkt in een bevraging over de acceptatie van specifieke technieken. Heel frequent wordt deze vraag gesteld in relatie tot de camerabewaking (Vermeersch & De Pauw, 2017; Mitrou, Drogkaris & Leventakis, 2018, Biesiot, de Bakker, Jacquemard & van Est, 2018…). Af en toe komt de acceptatie van specifieke biometrische technieken ter sprake, zoals bij Visser en Hoorweg (2018) en Biesiot, de Bakker, Jacquemard & van Est (2018). Als aanvulling op dit onderzoek wordt vervolgens specifiek onderzoek toegelicht dat ingaat op de acceptatie van biometrische technieken.

Uit een studie van de Verenigde Staten blijkt dat 87% van de Amerikanen de vingerafdruk als een legitiem identificatiemiddel beschouwd. 91% stelt dat de vingerafdruk een gerechtvaardigde techniek is voor toegangscontrole in hoog beveiligde gebieden en 76% zou het gebruiken in persoonlijke financiële procedures (Cehic & Quigley, 2005). Daarnaast blijkt uit een bevraging van 500 Amerikanen dat 40% van de respondenten geen idee heeft wat biometrische gegevens zijn (King, 2018).

Het draagvlak voor biometrie voor het bepalen van je identiteit wordt ook in Nederland door Visser en Hoorweg (2018) bestudeerd. Deze vraag wordt gesteld in relatie tot het vergroten van de veiligheid. Er wordt in dit onderzoek bovendien ingegaan op het gebruik van gezichtsherkenning. Op een schaal van zeer positief tot zeer negatief vinden we bij onderstaande stellingen de volgende antwoorden:

- Biometrie voor het bepalen van je identiteit: 25% is zeer positief, 31% positief, 31% neutraal, 13% negatief en 5% zeer negatief.
- Camera's in de publieke ruimte met gezichtsherkenning: 30% antwoordt zeer positief, 34% positief, 24% neutraal, 9% negatief en 4% zeer negatief.

In België opteert één op de twee Belgen voor biometrie als alternatief voor wachtwoorden om toegang te krijgen tot hun online-accounts, dit blijkt uit een onderzoek van technologiebedrijf Unisys, waarbij 3500 consumenten bevraagd werden in zeven Europese landen. 6/10 Vond het veiliger dan wachtwoorden en 59% prefereert de vingerafdruk, 47% verkiest de irisscan, 27% prefereert gezichtsherkenning en 20% verkiest stemherkenning (Van Nuffel, 2017). Uit het onderzoek van Insites Consulting (2016) blijkt dat 52% van de Belgen klaar is om biometrische betaalmethodes te gebruiken. Dit betekent dat de helft van de Belgen voorstander is van het betalen met vingerafdrukherkenning of betalen met een selfie (Mastercard, 2019).

In Duitsland bestuderen Krupp, Rathgeb & Busch 'the social acceptance of biometric technologies in Germany' door middel van een survey bij 140 burgers (Krupp, Rathgeb & Busch, 2013). Uit hun onderzoek blijkt dat een gemiddelde respondent zo'n 7 passwoorden onthoudt en zowel passwoorden als PIN's frequent vergeet. De meerderheid verandert bovendien de PIN's of passwoorden niet regelmatig. "*Based on these results, knowledge based-authentication systems requiring PINs or passwords appear inconvenient*". Biometrische systemen worden onder meer omwille van die redenen als oplossing aangeboden. De meest gekende systemen onder de respondenten zijn deze van vingerafdrukken, iris, face en speaker/voice recognition. Naast de kennis over de systemen worden door Krupp et al. (2013) evenzeer vragen gesteld naar de aanvaarding hiervan. De hoogste graad van acceptatie is er voor vingerafdrukherkenning, tevens de meest gekende vorm van technologie. Daarnaast blijkt dat hoe meer een technologie wordt gebruikt, hoe meer dit sociaal wordt aanvaard. Echter stellen Krupp et al. vast dat hoewel vormen zoals face, speaker en voice recognition gekend zijn, deze technologieën slechts door enkelen worden aanvaard en door 25% helemaal niet wordt aanvaard. De opgesomde nadelen betreffen het feit dat dit als te persoonlijk, intiem en zelfs als beangstigend wordt omschreven. Ongeveer 75% is ervan overtuigd dat biometrische toegangscontrolesystemen noodzakelijk zijn voor welbepaalde plaatsen. Tot slot wordt de vraag gesteld of men de toekomst positief inschat voor biometrische technologieën. Ongeveer 45% van de respondenten ziet de toekomst positief.

El-Abed, Giot, Hemery & Rosenberger (2012) bestuderen evenzeer dit onderwerp. Op basis van internationale literatuur stellen zij vast dat er heel wat tekortkomingen zijn in onderzoek. Dit noopte El-Abed et al. (2012) tot het bestuderen van de aanvaarding van de gebruikers en de tevredenheid over de biometrische systemen. Zij onderzoeken dit door een 'modality-independent evaluation methodology', waarbij er naast statistische data ook ruimte wordt gelaten aan de respondent om te verklaren waarom hij/zij een bepaalde mening is toegedaan. Door middel van een survey wordt data verzameld over socio-demografische factoren, 'learnability and memorability', vertrouwen, gebruiksvriendelijkheid, privacy, fysische invasiviteit en culturele aspecten.

De bevraagde respondenten vinden dat biometrisch gebaseerde technologieën beter zijn dan 'secret-based solutions' tegen fraude. Zowel het 'keystroke system' als de biometrisch-gebaseerde technologieën worden aanvaard waarbij 88,9% tevreden is over het eerste system en 75,8% tevreden is over biometrische technologieën. Hetgeen dat de mate van aanvaarding en tevredenheid beïnvloedt, heeft vooral te maken met: de robuustheid van het systeem om zich te beschermen tegen aanvallen, de gebruiksvriendelijkheid en de tijdsbesteding om iets te verifiëren (El-Abed, Giot, Hemery & Rosenberger, 2012).

Ada Lovelace institute bevroeg 4109 volwassenen over facial recognition (Ada Lovelace Institute, 2019). Op de vraag "*Identity verification is when a device uses either a password or biometrics (personal characteristics like fingerprints) to identify you as the device's owner. Which of the following methods of identity verification are you aware of? Please select all that apply*" duidt 87% vingerafdrukken aan, 74% face recognition, 68% voice recognition en 67% iris recognition.

Burgers zijn zich in grote mate bewust van deze technologie, echter is de kennis ontoereikend. 53% van de respondenten is zich bewust dat facial recognition bestaat en weet er iets van af. Dit betekent dat de helft van de respondenten zich hier niet bewust van is en 10% zich hier helemaal niet bewust van is. Bovendien weten heel wat burgers niet dat gelaatsherkenning ook door andere instanties dan politie of op de luchthaven wordt gebruikt. Minder dan 15% weet dat dit bestaat in bedrijven, winkels of andere commerciële aangelegenheden. Ada Lovelace institute raadt in zijn rapport aan om deze kennis te verhogen.

Een tweede vraag die wordt gesteld betreft "*And which of the following do you personally use/would be comfortable using to identify yourself on a mobile or other device? Please select one option per row*". De antwoorden zijn weergegeven in onderstaande tabel.

	Fingerprints	Iris/eye scanning	Voice recognition	Facial recognition/face scanning
N =	3584	2768	2785	3029
I personally use this method of identification	54%	4%	10%	15%
I do not use this method currently but would be comfortable doing so	29%	62%	45%	46%
I am not comfortable with using this method of identification	13%	27%	39%	32%
Don't know	4%	7%	7%	6%

Tabel 4: "*And which of the following do you personally use/would be comfortable using to identify yourself on a mobile or other device?"* (Ada Lovelace institute, 2019)

In bovenstaande tabel merken we op dat het persoonlijk gebruik van vingerafdrukken als identificatiemethode het vaakst voorkomt. Als er ingezoomd wordt op het antwoord "*I am not comfortable with using this method of identification*" dan polst deze vraag naar een bepaalde mate van aanvaardbaarheid van deze methode. De vingerafdrukken scoren het laagst: 13% heeft hier een oncomfortabel gevoel bij. Bijna 40% duidt dit antwoord aan bij 'voice recognition' en 32% vinkt dit aan bij facial recognition. Vingerafdrukken worden meer aanvaard dan andere biometrische technieken.

46% van de burgers uit de UK vindt dat ze de mogelijkheid moet krijgen om te kiezen of de toestemming te geven als facial recognition technologie wordt gebruikt. "*Survey respondents from black, Asian and minority ethnic groups are more likely to agree with the notion that the public should have the opportunity to consent*" (Ada Lovelace institute, 2019). Mensen zijn bezorgd over de toenemende surveillantie omdat technologieën zoals facial recognition in stijgende mate worden geïmplementeerd. Ze zijn echter bereid om dit te aanvaarden als deze technologie een aantoonbaar publiek voordeel oplevert. Zo vindt men het gebruik van facial recognition toelaatbaar door de politie bij crimineel onderzoek (70%), op smartphones om systemen te 'unlocken' (50%) in de veronderstelling dat er afdoende beveiliging is. De reden voor dit hoog percentage bij de politie heeft te maken met het feit dat men van mening is dat dit ten goede komt van de veiligheid van de

samenleving. In supermarkten, scholen, bedrijven… vindt men dit veel minder toelaatbaar. Zo is 67% *uncomfortable* met het gebruik van facial recognition in scholen en voelt 61% zich niet comfortabel met het gebruik hiervan op publiek transport.

Niettemin geeft 1/3de aan een oncomfortabel gevoel te krijgen bij de idee dat de politie facial recognition gebruikt. Zij geven hiervoor verschillende redenen zoals:

- 68% "*It infringes on the privacy of people in society*"
- 68% "*It normalizes surveillance*"
- 62% "*I can't opt out or consent*"
- 60% "*I do not trust them to use the technology ethically*" (Ada Lovelace institute, 2019).

Deze acceptatie is echter gelimiteerd, zo verwacht de burger regulering door de overheid. Verder verwacht men dat er bepaalde limieten worden gesteld aan het politioneel gebruik van facial recognition. 55% vindt dat de overheid de politie moet begrenzen in het gebruik ervan in specifieke omstandigheden.

Bedrijven die facial recognition gebruiken voor commerciële voordelen, worden in veel mindere mate aanvaard. Zo is 77% oncomfortabel met de idee dat facial recognition gebruikt wordt door winkels om consumenten te 'tracken' en voelt 76% zich niet comfortabel dat deze technologie wordt aangewend voor Human Resources doeleinden, zoals rekrutering. Het doel waarom facial recognition gebruikt wordt, is dus van groot belang. Het publieke belang – zoals het verhogen van de veiligheid of de bescherming – is veel fundamenteler voor de burger in het acceptatieproces van facial recognition dan het commerciële belang.

Tot slot is er een belangrijke rol weggelegd voor de overheid en de burger. De overheid kan de burger educeren en dialoog stimuleren maar er wordt hen ook een cruciale rol toebedeeld in het reguleren. Ada Lovelace Institute (2019) stelt evenzeer de burger centraal in dit hele debat en wenst publieke consultatie te stimuleren door een "*Citizens' Biometric Council, a citizen's assembly supported by the Information Commissioner's Office*".

5.7 Beschrijvende onderzoeksresultaten biometriesurvey

5.7.1 Quid België?

In navolging van bovenstaande onderzoeken stelde Vias institute een bevraging op omtrent de aanvaarding van biometrische technieken als vorm van toegangscontrole. De kopie van de vragenlijst bevindt zich in de bijlage.

In de literatuur wordt frequent het belang van kennis beschreven – in het proces van aanvaarding – waardoor de eerste vraag een kennisvraag betreft. Namelijk in hoeverre kent u de opgesomde identificatietechnieken? Vervolgens wordt gevraagd naar de aanvaardbaarheid van bepaalde technieken als vormen van toegangscontrole. We stellen ook specifieke en concrete vragen over de plaatsen waartoe men via de vingerafdruk toegang zou kunnen krijgen. We stellen deze vragen in functie van de vingerafdruk omdat uit de literatuur blijkt dat deze techniek het best gekend en dus meest aanvaard is.

Een meer algemene vraag wordt gesteld over de mate waarin specifieke sectoren technologie kunnen aanwenden. In bovenstaande literatuurstudie blijkt er immers meer acceptatie te zijn voor de implementatie van technologie in publieke sectoren in vergelijking met private sectoren.

Het opmaken van deze vragenlijst wordt in grote mate geïnspireerd vanuit de wetenschappelijk literatuur en/of onderzoek. In onze vragenlijst wordt ervoor gekozen om niet aan 'framing' te doen, dit wil zeggen dat de vragen zo neutraal mogelijk gesteld worden. Een laatste vraag gaat wel in op één van boven aangehaalde 'frames' in en haakt aan op de meest frequent aangehaalde reden waarom biometrische technieken niet 'mogen' toegepast worden, namelijk de privacy. De vraag 'In hoeverre bent u bereid om privacy in te ruilen voor meer veiligheid' sluit de vragenlijst af.

Met onze vragenlijst wensen we een accuraat, actueel en Belgisch beeld te schetsen van wat de kennis is van de burger over biometrische technieken, wat de aanvaardbaarheid is van de aanwending van deze technieken als toegangscontrole, op welke plaatsen een toegang via vingerafdrukken wenselijk is, welke sectoren welke technologie mogen aanwenden en in hoeverre men privacy wil inruilen voor meer veiligheid. Deze kennis

wordt tot dusver niet op deze wijze verzameld in België, waardoor er sprake is van een zekere mate van uniciteit.

5.7.2 Methodologie

5.7.2.1 Steekproef en foutenmarge

1000 Belgen worden bevraagd over de toepassing van verschillende biometrische technieken. Voor het trekken van de steekproef en de afname van de vragenlijst wordt er samengewerkt met iVOX. iVOX beschikt over een online onderzoekspanel in België bestaande uit 150000 leden. Er wordt een representatieve steekproef getrokken waarbij 1000 volwassen Belgen worden bevraagd.

De steekproeven worden *interlaced* getrokken via de zogenaamde getrapte toeval-steekproeven en door middel van een *propensity* weging. Door middel van deze weging wordt een garantie gegeven dat de juiste respondenten *random* gekozen worden. iVOX monitort de antwoorden op kwaliteit zoals invultijd, consistentie in de antwoorden waardoor de kwaliteit van de data wordt verzekerd. De respondenten die data van lage kwaliteit leveren worden uit het panel verwijderd. De foutenmarge van de resultaten wordt bepaald door de grootte van de steekproef enerzijds en de graad van betrouwbaarheid die men wenst anderzijds. De maximale foutenmarge bij 1000 Belgen bedraagt 3,02%.

5.7.3 Onderzoeksresultaten

5.7.3.1 Onderzoekspopulatie

Op basis van deze methodologie komen we tot een representatieve steekproef. 589 respondenten zijn Nederlandstalig (58,9%) en 411 respondenten (41,1%) zijn Franstalig. 49,6% is mannelijk en 50,4% vrouwelijk. Wat betreft de leeftijden ziet de verdeling er als volgt uit: 28,5% is tussen de 18 en 34 jaar, 36,7% tussen de 35 en 54 jaar en 34,8% is ouder dan 55 jaar. 64,7% volgde hoogstens middelbaar onderwijs terwijl 35,3% hoger onderwijs heeft gevolgd. Qua verdeling van de regio komt 57,9% van de respondenten uit Vlaanderen, 31,8% uit Wallonië en 10,3% uit Brussel.

5.7.4 Kennis

Het gebruik van biometrische identificatietechnieken duikt meer en meer op in onze huidige technologische samenleving. Door middel van deze technieken worden lichaamskenmerken van een persoon gemeten of vastgesteld (zoals vingerafdrukken, het gelaat, de iris…) en herkend. Een eerste vraag peilt naar de kennis van de respondenten over deze technieken.

Welke van onderstaande identificatietechnieken kent u?	Antwoordmogelijkheden	Aantal antwoorden	Percentage antwoorden
Vingerafdrukken	Ken ik en ik weet wat het juist inhoudt	854	**85,4%**
	Heb ik al van gehoord, maar ik weet niet wat het juist inhoudt	126	12,6%
	Ken ik niet	20	2,0%
	N=	1000	100,0%
Gelaatsherkenning			
	Ken ik en ik weet wat het juist inhoudt	682	**68,2%**
	Heb ik al van gehoord, maar ik weet niet wat het juist inhoudt	256	25,6%
	Ken ik niet	61	6,1%
	N=	100	100,0%
Irisherkenning			
	Ken ik en ik weet wat het juist inhoudt	643	**64,3%**
	Heb ik al van gehoord, maar ik weet niet wat het juist inhoudt	217	21,7%
	Ken ik niet	141	14,1%
	N=	1000	100,0%
Handafdrukherkenning			
	Ken ik en ik weet wat het juist inhoudt	432	**43,2%**
	Heb ik al van gehoord, maar ik weet niet wat het juist inhoudt	268	26,8%
	Ken ik niet	300	30,0%
	N=	1000	100,0%
Spraak-/stemherkenning	Ken ik en ik weet wat het juist inhoudt	667	**66,7%**
	Heb ik al van gehoord, maar ik weet niet wat het juist inhoudt	285	28,5%
	Ken ik niet	48	4,8%
	N=	1000	100,0%

Tabel 5: Welke van onderstaande identificatietechnieken kent u? (N=1000)

In bovenstaande tabel lezen we af dat de meest gekende identificatietechniek deze van de vingerafdrukken is. 85,4% van de respondenten duidt aan dat zij deze identificatietechniek kent en weet wat het inhoudt. De tweede meest gekende techniek is gelaatsherkenning. 68,2% kent gelaatsherkenning en weet wat het juist inhoudt. 25,6% hoorde er al van maar niet weet wat dit juist inhoudt. 66,7% kent de techniek van spraak/-stemherkenning en weet wat het juist inhoudt. 64,3% kent irisherkenning en weet wat het inhoudt, terwijl 21,7% hier al van gehoord heeft maar weet niet wat het inhoudt. De minst gekende techniek is de handafdrukherkenning: 30% kent dit niet.

Indien deze antwoorden gekruist worden met de achtergrondvragen worden enkele significante verbanden gevonden. Zo vinden we een significant verband[9] terug bij de *taalkeuze*. 76,1% van de Franstalige Belgen kent gelaatsherkenning en weet wat dit juist inhoudt ten opzichte van 62,8% Nederlandstalige Belgen. Het aantal Nederlandstalige Belgen dat de techniek van handafdrukherkenning kent, weet wat het inhoudt (46,3%) of er al van gehoord heeft maar niet weet wat het inhoudt (30,2%) ligt significant hoger dan de Franstalige Belgen (38,6% en 22%). Bij het antwoord 'ik ken het niet' vinden we een significant verband waarbij de Franstaligen dit in 39,4% van de gevallen aanduiden ten opzichte van 23,4% Nederlandstaligen. We vinden

[9] Significantie betekent niet louter toevallige verschillen (bij een betrouwbaarheidsniveau van 95%).

tot slot bij spraak/stemherkenning een significant verband waarbij de Franstalige Belgen in 73% van de gevallen aanduiden dat zij dit kennen en weten wat het inhoudt, ten opzichte van 62,3% Nederlandstaligen.

Wat betreft *geslacht* vinden we bij irisherkenning een significant verband terug waarbij de mannen in 69,1% van de gevallen aanduiden dat zij dit kennen en weten wat het inhoudt. Bij de vrouwen kent 59,5% deze techniek.

Bij iedere techniek worden significante verbanden gevonden indien deze techniek gekruist wordt met de */eeftijd*. De significante verbanden worden per techniek en per leeftijdscategorie weergegeven in bold.

		Leeftijd		
		<=34	35-54	55+
		(A) 285	(B) 367	(C) 348
Welke van onderstaande identificatietechnieken kent u?				
Vingerafdrukken	(N=)	285	367	348
	Ken ik en ik weet wat het juist inhoudt	**91.9% B C**	83,5%	82,1%
	Heb ik al van gehoord, maar ik weet niet wat het juist inhoudt	6,9%	**13.9% A**	**15.9% A**
	Ken ik niet	1,2%	2,6%	2,0%
Gelaatsherkenning	(N=)	285	367	348
	Ken ik en ik weet wat het juist inhoudt	**78.2% C**	**70.1% C**	58,1%
	Heb ik al van gehoord, maar ik weet niet wat het juist inhoudt	15,7%	**24.8% A**	**34.6% A B**
	Ken ik niet	6,1%	5,1%	7,3%
Irisherkenning	(N=)	285	367	348
	Ken ik en ik weet wat het juist inhoudt	**73.1% C**	**69.8% C**	51,2%
	Heb ik al van gehoord, maar ik weet niet wat het juist inhoudt	15,7%	20,9%	**27.4% A**
	Ken ik niet	11,2%	9,3%	**21.5% A B**
Handafdrukherkenning	(N=)	285	367	348
	Ken ik en ik weet wat het juist inhoudt	**50.8% C**	**47.2% C**	32,7%
	Heb ik al van gehoord, maar ik weet niet wat het juist inhoudt	21,6%	28,4%	29,5%
	Ken ik niet	27,6%	24,4%	**37.8% A B**
Spraak-/stemherkenning	(N=)	285	367	348
	Ken ik en ik weet wat het juist inhoudt	**77.2% C**	**69.0% C**	55,7%
	Heb ik al van gehoord, maar ik weet niet wat het juist inhoudt	19,0%	26,8%	**38.1% A B**
	Ken ik niet	3,9%	4,2%	6,2%

Tabel 6: Significante verbanden= kennis techniek - leeftijdscategorie

91,9% van de respondenten dat jonger is dan 34 jaar kent de techniek van vingerafdrukken en weet wat dit juist inhoudt terwijl deze percentages beduidend lager liggen bij de twee andere leeftijdscategorieën (83,5% en 82,1%). 13,9% van de 35 tot 54-jarigen en 15,9% van de 55-plussers duidt 'heb ik al van gehoord maar ik weet niet wat het juist inhoudt' aan terwijl slechts 6,9% van de 18 tot 34-jarigen dit aanduidt. Bij gelaatsherkenning vinden we evenzeer een significant verband bij de respondenten tussen 18 en 34 jaar (78,2% kent dit en weet wat het juist inhoudt) en tussen 35 en 54 jaar (70,1% kent dit en weet wat het juist

inhoudt) ten opzichte van 58,1% van de 55-plussers. We merken een significant verband op waarbij 73,1% van respondenten tussen 18 en 34 jaar en 69,8% tussen de 35 en 54 jaar irisherkenning kent en weet wat het inhoudt ten opzichte van 51,2% van de 55-plussers. 50,8% van de 18 tot 34-jarigen kent de techniek van handafdrukherkenning en weet wat het juist inhoudt, 47,2% van de 35 tot 54-jarigen duidt eenzelfde antwoord aan wat significant verschilt met de antwoorden van de 55-plussers. Tot slot wordt er bij spraak- en stemherkenning een significant verband gevonden: 18-34 jarigen (77,2%) en 35-54 jarigen (69,0%) duiden aan dat ze dit kennen en weten wat het inhoudt terwijl net iets meer dan de helft van de 55-plussers (55,7%) dit kent en weet wat het inhoudt.

Indien de antwoordcategorieën gekruist worden met het *diploma* stellen we enkele significante verbanden vast. Bij de vingerafdrukken vinden we een eerste significant verband waarbij hoger opgeleiden (hoger onderwijs) frequenter deze techniek kennen en weten wat het inhoudt (90,1% tov 82,9%). Eenzelfde significant verband vinden we terug bij gelaatsherkenning waarbij 28,5% van de respondenten dat hoogstens middelbaar onderwijs genoot al gehoord heeft van de techniek maar niet weet wat het inhoudt ten opzichte van 20,5% hoger opgeleiden. Deze laatste groep geeft in 72,9% van de gevallen aan dat zij irisherkenning kent en weet wat het inhoudt ten opzichte van 59,6% van de lager opgeleiden. Tot slot kent 73,2% van de hoger opgeleiden spraak/stemherkenning en weet zij wat dit inhoudt ten opzichte van 63,2% van de personen die hoogstens middelbaar onderwijs genoten.

Als we de kennisvraag kruisen met de *regio* vinden we een significant verband bij gelaatsherkenning waarbij de respondenten van Wallonië (76,6%) en Brussel (75,0%) het systeem van gelaatsherkenning beter kennen en weten wat het inhoudt ten opzichte van de respondenten uit Vlaanderen (62,4%). Voor de andere antwoordcategorieën treffen we een significant verband aan bij de Vlamingen: 29,5% van de Vlamingen heeft hier al van gehoord maar weet niet echt wat dit inhoudt (ten opzichte van 20,8% Walen). 8,1% Vlamingen kent de biometrische techniek van gelaatsherkenning niet terwijl dit 2,6% is van de Walen. Respondenten uit Wallonië en Vlaanderen kennen beduidend minder de techniek van handafdrukherkenning: zo duidt 37,1% Walen 'ken ik niet' aan, 44,4% van de Brusselaars 'ken ik niet' aan terwijl dit slechts 23,5% van de Vlamingen is. Aangaande spraak/- en stemherkenning gaan personen uit Wallonië – 72,2% - vaker 'ken ik en ik weet wat het juist inhoudt' aanduiden ten opzichte 62,6% van de Vlamingen. Deze laatste duiden vaker (32,8%) 'heb ik al van gehoord maar ik weet niet wat het juist inhoudt' aan ten opzichte van 23,3% Walen en 19,9% Brusselaars.

5.7.5 Aanvaarding van identificatietechnieken als toegangscontrole

De vraag wordt gesteld aan de respondenten in hoeverre ze onderstaande identificatietechnieken aanvaardbaar vinden als toegangscontrole.

	Helemaal niet aanvaard baar	Niet aanvaard baar	Eerder niet aanvaard baar	Eerder wel aanvaard baar	Wel aanvaard baar	Helemaal wel aanvaard baar
Vingerafdrukken (herkent een afdruk van een vinger)	3,9%	2,9%	6,2%	25,8%	30,9%	30,2%
Gelaatsherkenning (herkent het gelaat)	5,8%	7,7%	13,9%	27,8%	25,4%	19,4%
Irisherkenning (herkent een iris van het oog)	5,9%	5,1%	12,4%	26,9%	27,2%	22,4%
Handafdrukherkenning (herkent een handafdruk)	6,0%	5,6%	12,9%	29,9%	25,9%	19,7%
Spraak-/stemherkenning (herkent spraak of stem)	6,6%	9,1%	17,8%	29,0%	21,8%	15,7%

Tabel 7: In welke mate vindt u de identificatietechniek aanvaardbaar als vorm van toegangscontrole? (N=1000)

In bovenstaande tabel lezen we de antwoorden omtrent de mate van aanvaardbaarheid van verschillende toegangscontroletechnieken. In volgende tabel wordt de mate van aanvaardbaarheid geclusterd tot twee categorieën, namelijk 'niet aanvaardbaar' en 'wel aanvaardbaar'.

	Niet aanvaardbaar	Wel aanvaardbaar
Vingerafdrukken (herkent een afdruk van een vinger)	13,0%	87,0%
Gelaatsherkenning (herkent het gelaat)	27,4%	72,6%
Irisherkenning (herkent een iris van het oog)	23,5%	76,5%
Handafdrukherkenning (herkent een handafdruk)	24,5%	75,5%
Spraak-/stemherkenning (herkent spraak of stem)	33,5%	66,5%

Tabel 8: Antwoordcategorieën van tabel 2 geclusterd naar 'niet aanvaardbaar' en 'wel aanvaardbaar' (N=1000)

De aanvaardbaarheid voor de vingerafdrukken als vorm van toegangscontrole is het hoogst. Bijna negen op tien (87%) respondenten vindt het 'wel tot helemaal wel aanvaardbaar' dat vingerafdrukken als vorm van toegangscontrole worden gebruikt. De tweede meest aanvaardbare techniek betreft irisherkenning waarbij 76,5% dit aanvaardbaar vindt en 23,4% dit niet aanvaardbaar vindt. 75,5% aanvaardt handafdrukherkenning als vorm van toegangscontrole terwijl 24,5% dit niet aanvaardt. 72,6% vindt gelaatsherkenning aanvaardbaar en 27,4% vindt dit niet aanvaardbaar als vorm van toegangscontrole. De minst aanvaardbare vorm van toegangscontrole is spraak/stemherkenning waarbij 66,5% dit aanvaardt als identificatietechniek en 33,5% dit niet aanvaardt.

We kruisen vervolgens de vragen met een aantal achtergrondvragen en treffen enkele significante verbanden aan, onder andere bij de *taalkeuze*. Zo vindt 29,8% Nederlandstalige Belgen gelaatsherkenning niet aanvaardbaar ten opzichte van 24% Franstaligen. De Franstaligen zijn het meer eens over de aanvaardbaarheid van de gelaatsherkenning – namelijk 76% - in vergelijking met de Nederlandstaligen (namelijk 70,2%).

De mate van aanvaarbaarheid kruisen met *geslacht* levert enkele verbanden op. 89,9% van de vrouwen vindt de identificatietechniek van vingerafdrukken aanvaardbaar ten opzichte van 83,9% van de mannen. Ook bij de handafdrukherkenning treedt een gelijkaardige significantie op, met name 78,2% vrouwen vindt dit aanvaardbaar terwijl dit 72,8% van de mannen betreft. Er treedt evenzeer een significant verband op bij de niet aanvaardbaarheid waarbij mannen dit meer aanduiden dan vrouwen (27,2% mannen en 21,8% vrouwen).

Bij het kruisen van deze vraag met de achtergrondvariabele *leeftijd*, merken we dat de respondenten onder de 54 jaar (31,1% 18 tot 34-jarigen en 28,5% 35 tot 54-jarigen) vingerafdrukken vaker 'eerder wel aanvaardbaar' vinden in vergelijking met 55-plussers (18,8%). Deze laatste groep komt sterk naar voor (39,6%) bij de score 'helemaal wel aanvaardbaar' terwijl de leeftijdscategorie onder de 54 jaar ongeveer 25% in beslag neemt. Eenzelfde significant verband treedt op bij de irisherkenning. 27,9% van de 55-plussers acht irisherkenning 'helemaal wel aanvaardbaar' als vorm van toegangscontrole (ten opzichte van 18,8% van de 18 tot 34-jarigen en 20,2% van de 35 tot 54-jarigen).

Bij het kruisen van de mate van aanvaarding met het *diploma* vinden we tot slot een significant verband bij de spraak/stemherkenning: 37,9% dat hoger onderwijs volgde, duidt 'niet aanvaardbaar' aan terwijl dit 31,2% is van diegenen die hoogstens middelbaar onderwijs volgden. Dezelfde personen vinden het in 68,8% van de gevallen aanvaardbaar ten opzichte van 62,1% in hoger onderwijs.

5.7.6 Bereidheid tot het geven van een vingerafdruk om toegang te krijgen tot specifieke plaatsen

	Helemaal niet bereid	Niet bereid	Eerder niet bereid	Eerder wel bereid	Wel bereid	Helemaal wel bereid
In het bedrijf waar ik werk	13,7%	6,5%	8,7%	24,6%	23,9%	22,6%
In een bedrijf waar anderen werken	14,9%	10,0%	15,7%	21,6%	19,2%	18,5%
In de sportclub	18,8%	12,0%	14,1%	22,9%	16,9%	15,3%
In een voetbalstadion of dergelijke	19,1%	8,4%	11,2%	24,4%	18,7%	18,2%
Op een muziekfestival	19,8%	10,1%	13,1%	21,7%	16,7%	18,6%
In onderwijsinstellingen	16,7%	9,3%	12,6%	24,7%	18,1%	18,6%
Op het openbaar vervoer zoals de trein, tram, metro, bus	21,0%	12,1%	17,4%	19,7%	14,8%	15,0%
Op de luchthaven	12,0%	7,8%	11,0%	24,1%	21,1%	24,0%
In het shoppingcentrum	26,6%	16,5%	20,6%	14,0%	11,3%	11,1%
In een openbare parking	22,1%	14,1%	24,3%	15,0%	12,0%	12,5%
In een private parking	17,2%	10,5%	16,0%	23,2%	16,8%	16,3%
In een financiële instelling	14,8%	8,6%	13,1%	24,7%	19,7%	19,1%
In mijn woning	16,8%	7,9%	12,0%	21,2%	20,2%	21,9%
Om mijn smartphone te ontgrendelen	7,3%	4,7%	6,6%	21,8%	26,4%	33,2%

Tabel 9: In hoeverre bent u bereid om via uw vingerafdruk toegang te krijgen tot de volgende plaatsen? (N=1000)

In bovenstaande tabel vinden we cijfergegevens over de mate van bereidheid om vingerafdrukken af te geven op specifieke plaatsen. In onderstaande tabel wordt de mate van bereidheid geclusterd in de categorieën 'wel bereid' en 'niet bereid' per plaats.

	Niet bereid	Wel bereid
In het bedrijf waar ik werk	28,9%	71,1%
In een bedrijf waar anderen werken	40,6%	59,4%
In de sportclub	44,9%	55,1%
In een voetbalstadion of dergelijke	38,7%	61,3%
Op een muziekfestival	43,0%	57,0%
In onderwijsinstellingen	38,6%	61,4%
Op het openbaar vervoer zoals de trein, tram, metro, bus	50,5%	49,5%
Op de luchthaven	30,7%	69,3%
In het shoppingcentrum	63,7%	36,3%
In een openbare parking	60,5%	39,5%
In een private parking	43,7%	56,3%
In een financiële instelling	36,5%	63,5%
In mijn woning	36,7%	63,3%
Om mijn smartphone te ontgrendelen	18,6%	81,4%

Tabel 10: Antwoordcategorieën van tabel 6 geclusterd naar 'niet bereid' en 'wel bereid' (N=1000)

In bovenstaande tabel vinden we verschillende locaties terug waar men bereid is om via zijn vingerafdrukken toegang te krijgen tot een aantal plaatsen. De hoogste score 'wel bereid' vinden we bij 81,4% van de respondenten voor het ontgrendelen van de smartphone. 18,6% van de respondenten geeft aan hier niet toe bereid te zijn.

Als de antwoorden gekruist worden met de achtergrondvariabelen vinden we enkele significante verbanden. Een eerste significant verband vinden we bij de *taalkeuze*: 32,3% Franstalige Belgen is niet bereid om via vingerafdrukken de toegang te krijgen tot het 'bedrijf waarin men zelf werkt' ten opzichte van 26,6% Nederlandstaligen. Wat betreft de sportclub is 48,9% Franstaligen niet bereid om via vingerafdrukken toegang te krijgen ten opzichte van 42,2% Nederlandstaligen. De niet-bereidheid tot geven van vingerafdrukken als vorm van toegangscontrole op de luchthaven is groter bij de Nederlandstaligen (34,2%) dan bij Franstaligen (25,9%). Een laatste significant verband wordt gevonden bij de eigen woning waarbij 40,3% Franstaligen (ten opzichte van 34,2% Nederlandstaligen) niet bereid is om via vingerafdrukken toegang te krijgen.

Wat betreft *geslacht* is 21,8% van de mannen niet bereid om via zijn vingerafdruk de smartphone te ontgrendelen terwijl dit 15,4% van de vrouwelijke respondenten betreft. 84,6% vrouwen is wel bereid om zijn smartphone te ontgrendelen via de vingerafdruk ten opzichte van 78,2% van de mannen.

We vinden evenzeer significante verbanden als bovenstaande antwoorden worden gekruist met de *leeftijd*. De helft, namelijk 49%, van de 18 tot 34-jarigen is niet bereid om zijn vingerafdrukken af te geven als vorm van toegangscontrole 'in het bedrijf waar anderen werken' ten opzichte van 34,7% 55-plussers. 55-plussers zijn beduidend meer bereid (65,3%) om hun vingerafdrukken af te staan in 'het bedrijf waar anderen werken'. 52% van de 18 tot 34-jarigen is niet bereid om zijn vingerafdrukken te gebruiken in de sportclub, wat een hoger percentage is in vergelijking met dat van de 55-plussers (39,5%).

Het kruisen van de plaats 'in een voetbalstadion of dergelijke' met de leeftijd levert opnieuw een significant verband op: 45,3% van de 18 tot 34-jarigen is niet bereid om via zijn vingerafdruk toegang te krijgen tot 'een voetbalstadion of dergelijke'. Bijna 65% (64,9%) van de bevraagden die ouder zijn dan 55 jaar geeft aan bereid te zijn om via zijn vingerafdruk toegang te krijgen tot 'een voetbalstadion of dergelijke'. Iets meer dan de helft van de 18 tot 34-jarigen is niet bereid om via zijn vingerafdrukken toegang te krijgen tot een muziekfestival (bij de 35 tot 54-jarigen is dit 41,3% en 37,8% van de 55-plussers). Eenzelfde bereidwillige houding vinden we terug bij de onderwijsinstellingen: respondenten tussen 35 en 54 jaar (64,3%) en 55-

plussers (66,1%) zijn bereid om via hun vingerafdrukken een toegang te krijgen tot onderwijsinstellingen. Het hoogste aantal niet-bereidwilligen vinden we terug bij de jongste bevraagden.

60,5% van de 18 tot 34-jarigen is niet bereid om via vingerafdrukken toegang te krijgen tot het openbaar vervoer zoals de trein, tram, metro en bus. 50,9% van de 35 tot 54-jarigen is hier wel toe bereid en 56% van de 55-plussers is hier evenzeer toe bereid. Bijna 70%, namelijk 68,3%, van de respondenten tussen 18 en 34 jaar is niet bereid om via vingerafdrukken toegang te krijgen tot het shoppingcentrum. Diegenen die het meest bereid zijn om via vingerafdrukken toegang te krijgen tot een shoppincentrum zijn de 55-plussers, met name duidt 42,2% wel bereid aan (ten opzichte van 31,7% van de 18-34 jarigen).

Een gelijkaardig significant verband wordt gevonden bij de openbare parking waarbij 66,9% van de 18 tot 34-jarigen aangeeft niet bereid te zijn om via zijn vingerafdrukken toegang te krijgen tot de openbare parking. De 35 tot 54-jarigen zijn hier het meest toe bereid, namelijk 43,7%. Bij de private parking is er iets meer bereidheid: namelijk 60,5% van de 35 tot 54-jarigen en 58,4% van de 55-plussers is bereid om via zijn vingerafdruk toegang te krijgen tot een private parking.

Als deze bereidwilligheid gekruist wordt met het *diploma* is 57,9% van de respondenten dat hoogstens hoger middelbaar onderwijs genoot bereid om via zijn vingerafdrukken toegang te krijgen tot de sportclub ten opzichte van 49,9% van de respondenten dat hoger onderwijs volgde. Een significant verband wordt tevens gevonden bij het muziekfestival waarbij 49,6% van de respondenten dat hoger onderwijs volgde, aangeeft niet bereid te zijn om via vingerafdrukken toegang te krijgen tot een muziekfestival. Ook voor wat betreft het openbaar vervoer vinden we een significant verband en geven hoger opgeleiden in 55,3% van de gevallen aan dat ze niet bereid zijn om via een vingerafdruk toegang te krijgen tot het openbaar vervoer zoals de trein, tram, metro en bus ten opzichte van 48% van de respondenten dat hoogstens hoger middelbaar onderwijs volgde. 39,1% van de lager opgeleiden is tot slot niet bereid om via vingerafdrukken toegang te krijgen tot zijn woning ten opzichte van 32,4% van de hoger opgeleiden.

Het kruisen van de *regio* met de bereidwilligheid om via vingerafdrukken toegang te krijgen tot bepaalde plaatsen levert tot slot enkele verbanden op. Zo vinden we een significant verband terug bij de respondenten uit Vlaanderen: zij zijn bereid om via vingerafdrukken toegang te krijgen tot de sportclub. 58,1% van de Vlamingen is hiertoe bereid ten opzichte van 49,4% van de Walen. 34,7% van de Vlamingen geeft aan dat zij niet bereid is om via vingerafdrukken toegang te krijgen tot de luchthaven ten opzichte van 24,8% van de Walen.

5.7.7 Personen of organisaties die gebruik kunnen maken van biometrische technieken

De personen of organisaties die volgens de respondenten gebruik mogen maken van biometrische technieken staan weergegeven in onderstaande tabel.

Duid aan welke van de volgende personen of organisaties volgens u gebruik mogen maken van de opgesomde technieken	Camera's	Vingeraf drukken	Irisscans	Spraak/stem herkenning	Gelaatsher kenning	Geen van deze technieken
Politie	81,40%	80,10%	52,60%	48%	59,20%	3,80%
Private bewakingsbedrijven	72,20%	32,10%	20,40%	19,60%	28,00%	16,80%
Brandweer	70,40%	37,60%	26,00%	22,70%	29,60%	18,40%
Winkels en shoppingcentra	67,10%	12,10%	7,40%	6,00%	16,60%	24,30%
Openbare vervoersmaatschappijen	67,00%	21,40%	9,90%	9,00%	19,30%	22,80%
Medische diensten	63,40%	51,70%	36,00%	27,40%	35,10%	15,50%
Onderwijsinstellingen	61,60%	31%	14,00%	14,20%	22,10%	25,90%
Gewone burgers	40,60%	19,60%	9,10%	11,70%	12,60%	45,80%
Sociale media	19,60%	15,40%	6,70%	10,10%	12,20%	61,00%

Tabel 11: Het aantal respondenten dat aanduidt welke personen of organisaties gebruik kunnen maken van biometrische technieken (N=1000)

81,4% van de respondenten geeft aan dat de politie gebruik mag maken van camera's en 80,1% stelt dat de politie vingerafdrukken mag aanwenden als biometrische techniek. Volgens 59,2% mag de politie gebruik maken van gelaatsherkenning, 52,6% duidt irisscans aan die de politie mag gebruiken en 48% duidt spraakherkenning aan als techniek die de politie mag aanwenden. Opvallend is het bijzonder laag aantal respondenten dat 'geen van deze technieken' aanduidt bij de politie, namelijk 3,8%.

Camera's mogen volgens 72,2% gebruikt worden door private bewakingsbedrijven. De andere technieken, zoals vingerafdrukken, irisscan, spraak/stemherkenning en gelaatsherkenning worden minder aangeduid bij private bewakingsbedrijven. Net zoals bij de private bewakingsbedrijven, is het volgens 70,4% mogelijk dat camera's gebruikt worden door de brandweer. Over het aanwenden van de andere technieken door de brandweer is men het minder eens.

Zowel winkel- en shoppingcentra, als openbare vervoersmaatschappijen mogen volgens 67% van de respondenten camera's gebruiken. Over het aanwenden van andere biometrische technieken is men het beduidend minder eens.

Wat de medische diensten betreft, zien we dat 63,4% aangeeft dat zij gebruik mogen maken van camera's. Iets meer dan de helft van de respondenten, namelijk 51,7%, vindt dat de medische diensten vingerafdrukken mogen gebruiken, 36% vindt dat de irisscan kan gebruikt worden en 35,1% geeft aan dat gelaatsherkenning mag aangewend worden. Bijna 1/3de (27,4%) vindt dat spraak/stemherkenning mag aangewend worden door medische diensten. Net zoals bij de medische diensten geeft 61,6% aan dat camera's mogen gebruikt worden door onderwijsinstellingen. Volgens 31% mogen onderwijsinstellingen vingerafdrukken aanwenden. Aangaande het gebruik van de andere technieken door onderwijsinstellingen zijn beduidend meer respondenten het oneens. Volgens 25,9% mag 'geen van deze technieken' aangewend worden in onderwijsinstellingen.

40,6% vindt dat cameragebruik door gewone burgers mag terwijl dit percentage bij de overige technieken beduidend lager ligt. Eén van de hoogste percentages dat 'geen van deze technieken' aanduidt (namelijk 45,8%) vinden we hier terug. Tot slot duidt 61% aan dat sociale media 'geen van deze technieken' mag gebruiken. 19,6% vindt dat sociale media camera's mag gebruiken, 15,4% vingerafdrukken, 6,7% irisscans, 10,1% spraak/stemherkenning en 12,2% gelaatsherkenning.

Bovenliggende onderzoeksresultaten worden gekruist wat enkele significante verbanden oplevert. Er wordt een significant verband gevonden tussen de *taalkeuze* en de verschillende sectoren die camera's mogen gebruiken. Nederlandstalige respondenten zullen beduidend vaker dan Franstaligen aanduiden dat camera's mogen gebruikt worden door de politie, private bewakingsbedrijven, brandweer, winkels en shoppingcentra, openbare vervoersmaatschappijen en medische diensten. We vinden gelijkaardige significante verbanden bij de vingerafdrukken, de irisscan en spraakherkenning. Als laatste treffen we bij gelaatsherkenning een significant verband aan waarbij meer Nederlandstaligen in vergelijking met Franstaligen (39,9% vs 28,2%) vinden dat deze techniek kan aangewend worden door de medische diensten. Bij de antwoordmogelijkheid 'geen van deze technieken' vinden we een hoger percentage Nederlandstaligen terug bij sociale media (namelijk 65,5% tov 54,5% Franstaligen). De Franstaligen duiden vaker 'geen van deze technieken aan' voor wat betreft de brandweer, medische diensten en politie.

De antwoorden op deze vraag worden gekruist met de achtergrondvariabele *geslacht*. 42,2% van de vrouwen duidt aan dat vingerafdrukken door de brandweer mogen gebruikt worden (in vergelijking met 32,9% van de mannen). 23,6% van de mannen stelt dat gewone burgers vingerafdrukken mogen gebruiken ten opzichte 15,8% van de vrouwen terwijl 17,8% van de mannen vindt dat sociale media vingerafdrukken mogen aanwenden ten opzichte van 13,1% van de vrouwen. Aangaande de irisscan duiden mannen iets vaker aan dat gewone burgers (12,7%), winkels en shoppingcentra (9,2%) en sociale media (8,8%) hiervan gebruik mogen maken. We vinden evenzeer significante verbanden bij gelaatsherkenning waarbij vrouwen vaker aanduiden dat brandweer en private bewakingsbedrijven gebruik mogen maken van deze techniek in vergelijking met mannen. Sociale media mag deze techniek iets meer aanwenden volgens mannen, namelijk door 14,6%, in vergelijking met 9,8% van de vrouwen.

De *leeftijd* wordt gekruist met de vraag naar de aanwending van de technieken in bepaalde sectoren/plaatsen. Een eerste significant verband wordt opgemerkt bij de 35 tot 54-jarigen waarbij 45,8% aangeeft dat gewone burgers camera's mogen gebruiken ten opzichte van 36,9% 55-plussers. Bij de 'vingerafdrukken' zien we dat 36,2% van de 55-plussers het mogelijk acht dat dit door onderwijsinstellingen wordt gebruikt ten opzichte van 23,8% 18 tot 34-jarigen. Deze laatsten achten het meer mogelijk dat gewone burgers (26,4%) en sociale media (20%) vingerafdrukken gebruiken. Aangaande de irisscan geven de 35 tot 54-jarigen meer aan dat medische diensten deze techniek mogen aanwenden (namelijk 58,3%) in vergelijking met 55-plussers

(48,5%). Wat betreft spraak/stemherkenning stelt 18,3% 55-plussers dat onderwijsinstellingen deze techniek mogen gebruiken ten opzichte van 10,2% van de 18 tot 34-jarigen.

Gelaatsherkenning wordt door 65% van de 35 tot 54-jarigen als meer aannemelijk geacht voor politie ten opzichte van 54,1% van de 55-plussers. Deze laatste categorie, met 33,3%, vindt dat de brandweer dit mag gebruiken in vergelijking met 24,4% van de 18 tot 34-jarigen. De 35 tot 54-jarigen (23,9%) en de 55-plussers (28,5%) stellen dat gelaatsherkenning meer mag aangewend worden in onderwijsinstellingen in vergelijking met de jongste respondenten (18 tot 34 jaar: 12,1%). 22,8% van de 55-plussers vindt dat gelaatsherkenning gebruikt kan worden bij openbare vervoersmaatschappijen ten opzichte van 13,7% van de 18 tot 34-jarigen. Deze laatsten vinden tot slot dat gelaatsherkenning meer mag aangewend worden op sociale media (17,3% duidt dit aan) in vergelijking met de andere leeftijdscategorieën. Zo is dit slechts 8,3% van de 55-plussers. De antwoordmogelijkheid 'geen van deze technieken' wordt door 35-plussers vaker aangeduid bij sociale media.

Aangaande het kruisen met *diploma* vinden meer respondenten die hoogstens hoger middelbaar onderwijs volgden, namelijk 34,4%, dat private bewakingsbedrijven vingerafdrukken mogen aanwenden ten opzichte van 27,8% van de hoger opgeleiden. 21,9% van de lager opgeleiden acht het meer mogelijk dat gewone burgers vingerafdrukken gebruiken ten opzichte van 15,2% van de hoger opgeleiden. Aangaande de irisscan zien we dat 9% van de respondenten dat hoogstens hoger middelbaar onderwijs volgde het meer toelaatbaar acht dat winkels en shoppingcentra irisscans gebruiken in vergelijking met 4,5% van de hoger opgeleiden. Wat betreft gelaatsherkenning acht 21,2% van de lager opgeleiden het mogelijk dat openbare vervoersmaatschappijen gebruik maken van gelaatsherkenning ten opzichte van 15,9% hoger opgeleiden. 15,5% van de hoger opgeleiden stelt dat sociale media gebruik mogen maken van gelaatsherkenning ten opzichte van 10,4% lager opgeleiden. Bij de antwoordcategorieën 'geen van deze technieken' duiden de hoger opgeleiden (28,3%) dit vaker aan bij 'winkels en shoppingcentra' ten opzichte van lager opgeleiden (22,1%).

Tot slot worden significante verbanden gevonden indien de *regio* gekruist wordt met de biometrische techniek en de plaats. Zo duiden Vlamingen vaker dan Walen en Brusselaars aan dat politie, private bewakingsbedrijven, brandweer, openbare vervoersmaatschappijen en medische diensten camera's mogen gebruiken. Een gelijkaardig significant verband vinden we terug bij de vingerafdrukken. Dit verband duikt evenzeer op voor wat betreft het aanwenden van irisscans bij politie, medische diensten, brandweer, onderwijsinstellingen en gewone burgers: Vlamingen vinden dat deze diensten meer gebruik mogen maken van irisscans in vergelijking met Walen en Brusselaars. Bij spraak-/stemherkenning vinden we een significant verband waarbij iets meer Vlamingen dan Walen en Brusselaars aanduiden dat deze techniek bij politie en medische diensten mag worden toegepast. Een significant statistisch verband vinden we daarenboven bij gelaatsherkenning waarbij 40% van de Vlamingen aanhaalt dat de medische diensten deze techniek kan aanwenden ten opzichte van 28,7% van de respondenten uit Wallonië en 27,5% uit Brussel. Het antwoord 'geen van deze technieken' wordt in Wallonië iets meer aangeduid bij de brandweer en medische diensten in vergelijking met de Vlamingen.

5.7.8 Ruilen van privacy voor veiligheid

In hoeverre bent u bereid om privacy in te ruilen voor meer veiligheid?		
N=	1000	100%
Helemaal niet bereid	112	11,20%
Niet bereid	102	10,20%
Eerder niet bereid	210	21,00%
Eerder wel bereid	388	38,80%
Wel bereid	103	10,30%
Helemaal wel bereid	85	8,50%

Tabel 12: In hoeverre bent u bereid om privacy in te ruilen voor meer veiligheid? (N=1000)

De laatste vraag die gesteld wordt in deze survey betreft de vraag: "*In hoeverre bent u bereid om privacy in te ruilen voor meer veiligheid?*". Bovenstaande tabel geeft de mate van bereidheid weer en in onderstaande tabel worden de antwoorden geclusterd tot twee categorieën: 'niet bereid' en 'wel bereid'.

Bovenstaande antwoorden gehercodeerd naar 2 categorieën 'wel bereid' – 'niet bereid'			
In hoeverre bent u bereid om privacy in te ruilen voor meer veiligheid?	(N)	1000	100,0%
	Niet bereid	425	42,5%
	Wel bereid	575	57,5%

Tabel 13: In hoeverre bent u bereid om privacy in te ruilen voor meer veiligheid? Gehercodeerde antwoordcategorieën (N=1000)

De meerderheid van de respondenten is bereid om privacy in te ruilen voor meer veiligheid. Als we de scores 'helemaal niet bereid tot eerder niet bereid' clusteren tot 1 categorie, namelijk de niet-bereidwilligen dan is 42,5% hier niet toe bereid terwijl 57,5% bereid is om zijn privacy in te ruilen voor meer veiligheid. Van de bereidwilligen duidt 8,5% 'helemaal wel bereid' aan, 10,3% 'wel bereid' en 38,8% 'eerder wel bereid'. Daarentegen is 21% 'eerder niet bereid' om de privacy in te ruilen voor meer veiligheid, 10,2% 'niet bereid' en is 11,2% 'helemaal niet bereid' om zijn privacy in te ruilen voor meer veiligheid.

Het kruisen van deze resultaten met de achtergrondvariabelen genereert significante verbanden. Zo vinden we een eerste significant verband terug bij de *taalkeuze* waarbij Franstaligen vaker aanduiden dat ze niet bereid zijn om hun privacy in te ruilen voor meer veiligheid (52,5%) ten opzichte van Nederlandstaligen (64,5%) die meer bereid zijn om hun privacy in te ruilen voor veiligheid (tov 47,5% van de Franstaligen).

Het kruisen van deze vraag met de achtergrondvariabele *geslacht* levert evenzeer een significant effect op. Mannen zullen vaker 'helemaal niet bereid' aanduiden (14,8%) bij de vraag of men zijn privacy wenst in te ruilen voor meer veiligheid ten opzichte van vrouwen (7,8%). Vrouwen duiden iets vaker 'helemaal wel bereid' (10,7%) aan in vergelijking met mannen (6,3%) terwijl deze laatsten dan vaker 'wel bereid' aanduiden (12,9% mannen ten opzichte van 7,7% vrouwen).

Aangaande de *leeftijd* vinden we evenzeer een significant verband: 18 tot 34-jarigen zijn vaker 'niet bereid' om hun privacy in te ruilen voor meer veiligheid in vergelijking met 55-plussers. 55-plussers antwoorden vaker 'wel bereid' te zijn, (namelijk 63,6%) om hun privacy in te ruilen voor meer veiligheid ten opzichte van 18 tot 34-jarigen (namelijk 50,9%).

Respondenten die hoger onderwijs – cfr. *Diploma* - genoten zijn 'eerder niet bereid' om hun privacy te ruilen ten opzichte van meer veiligheid in vergelijking met de respondenten die hoogstens middelbaar onderwijs genoten.

Wat *regio* betreft zijn Vlamingen vaker 'wel bereid', namelijk 64%, om hun privacy in te ruilen voor meer veiligheid ten opzichte van de respondenten uit Wallonië (48,4%) en Brussel (49,6%).

Deze vraag wordt gekruist met de *geclusterde aanvaarbaarheidsscores* en levert significante verbanden op. We vinden bij personen die de vingerafdrukken niet aanvaarden (namelijk 13%) een significant verband met de niet-bereidwilligen om privacy in te ruilen tegen veiligheid (24,1%) ten opzichte van de bereidwilligen (namelijk 4,9%). 87% aanvaardt vingerafdrukken en dit levert een significant op bij het kruisen met de ruilvraag: met name 95,1% is bereid privacy te ruilen voor meer veiligheid ten opzichte van 75,9% niet-bereidwilligen. We vinden gelijkaardige verbanden terug bij de andere vormen van biometrie. Irisherkenning wordt door 76,5% aanvaard en door 23,5% niet aanvaard. Bij deze laatste antwoordcategorie treffen we meer niet-bereidwilligen aan in plaats van bereidwilligen (36% tov 14,2%). Bij de personen die irisherkenning aanvaarden vinden we tevens een significant verband bij de privacyruilvraag waarbij 85,8% bereid is om privacy te ruilen voor meer veiligheid ten opzichte van 64% dat hier niet toe bereid is. 75,5% aanvaardt handafdrukherkenning; de personen die bereid zijn om privacy in te ruilen voor meer veiligheid scoren hier significant hoger (87,3%) in vergelijking met deze die hier niet toe bereid zijn (59,6%). Bij de niet-aanvaarding van handafdrukherkenning scoren de niet-bereidwilligen hoger (40,4%) in vergelijking met de bereidwilligen (12,7%). Bij gelaatsherkenning vinden we dezelfde tendens. Respondenten die dit niet aanvaarden zijn meer niet bereid (46%) dan wel bereid (13,7%) om privacy te ruilen voor meer veiligheid. De bereidwilligen scoren significant hoger (86,3%) dan de niet-bereidwilligen (54%) bij het aanvaarden van gelaatsherkenning. Deze vaststelling geldt evenzeer voor spraak/stemherkenning waar 66,5% dit aanvaardt en 33,5% dit niet aanvaardt. De personen die niet bereid zijn om privacy te ruilen voor veiligheid (46,5%) (tov 24% bereidwilligen) zullen deze techniek niet aanvaarden. De personen die wel bereid zijn om privacy te ruilen voor veiligheid (76%) scoren significant hoger ten opzichte van de personen die dit niet willen (53,5%) én aanvaarden deze technologie. We nemen tot slot eenzelfde tendens waar per sector: de mate van aanvaarding van een biometrische techniek in een sector genereert eenzelfde significant verband met de mate waarin men

bereid is om privacy in te ruilen voor veiligheid. Zo duidt 81,4% aan dat de politie camera's mag aanwenden en merken we op dat de bereidwilligen significant hoger scoren dan de niet-bereidwilligen.

6 Terugkoppeling empirie met theorie

6.1 Onbekend maakt onbemind

Kennis is een belangrijke factor als het draagvlak van de bevolking ten aanzien van biometrische technieken wordt bestudeerd. Het Europese SurPRISE onderzoek (Pavone et al., 2015) toont aan dat wanneer burgers geïnformeerd worden over de aard van de technologie ze de Surveillance Oriented Security Technologies belangrijk en noodzakelijk vinden om de publieke veiligheid te waarborgen. Niettemin is er een bezorgdheid bij de burger omwille van een gebrekkige controle en informatie. Er worden vragen gesteld aangaande accountability en men vreest misbruik van macht of functie. Pavone et al. (2015) stellen vast dat burgers doorgaans weinig kennis hebben over technologische technieken wanneer zij zich een opinie vormen. Deze attitude wordt daarenboven vaak 'geframed' bevraagd, wat de onderzoeksresultaten beïnvloedt. Snijders et al. (2019) beamen het belang van kennis en concluderen dat de meer kritische vragen door hun deelnemers van de focusgroep worden gesteld bij onbekende technologieën. Koops & Vedder (2001), Dinev et al. (2005) bevestigen het belang van kennis, niet enkel over de techniek as such maar ook over wat er met de verzamelde informatie gebeurt en voor welk doel de informatie wordt ingezet.

Uit onze survey blijkt dat de kennis varieert per techniek. Er wordt bovendien een onderscheid gemaakt tussen 'kennis en effectief weten wat het inhoudt' en 'al van gehoord hebben maar niet weten wat het inhoudt'. De vingerafdrukken zijn de meest gekende techniek, waarbij maar liefst 85,4% beweert de techniek te kennen en weet wat het inhoudt. 12,6% heeft hier al over gehoord en slechts 2% kent dit helemaal niet. De tweede meest gekende techniek betreft gelaatsherkenning (68,2%) en derde meest gekende techniek is spraak- en stemherkenning (66,7%): beide technieken zijn door ongeveer 67% gekend (en waarbij men weet/beweert wat de techniek inhoudt). Ongeveer 5% kent dit helemaal niet, wat een beduidend lager percentage is indien we dit vergelijken met Amerikaans onderzoek van King waarbij 40% geen idee heeft wat biometrische gegevens zijn. De minst gekende techniek in ons onderzoek is deze van handafdrukherkenning waarbij 30% dit helemaal niet kent.

Net zoals in onze survey blijkt dat vingerafdrukken ook de meest gekende techniek is in de UK, namelijk 87% kent deze techniek. Verder vindt Ada Lovelace institute (2019) dat 74% kennis heeft over gelaatsherkenning, 68% kent spraak/stemherkenning en 67% kennis heeft over irisherkenning. In hun onderzoek zoomen zij specifiek in op facial recognition en stellen zij vast dat de kennis laag is. 10% is zich helemaal niet bewust van het bestaan van deze technologie, 36% is zich hier wel bewust van maar weet helemaal niets van deze technologie. Dit betekent dat de helft van de respondenten in de UK facial recognition niet kent. In België kent 68,2% dit en weet - al dan niet - wat het inhoudt. Dit is een hoger percentage in vergelijking met de UK.

Krupp, Rathgeb & Busch (2013) bestuderen de sociale acceptatie van biometrische technieken en stellen vast dat de meest gekende systemen deze van vingerafdrukken, iris, face en speaker/voice recognition zijn. De vingerafdrukherkenning is de meest gekende technologie, wat door onze onderzoeksresultaten bekrachtigd wordt.

6.2 Vingerafdrukken meest aanvaard

Uit onze bevraging blijkt dat 87% van de respondenten de vingerafdruk – als vorm van toegangscontrole – aanvaardt. Deze aanvaarding is er evenzeer voor de andere technieken maar in iets mindere mate. Zo aanvaardt 76,5% irisherkenning, 75,5% handafdrukherkenning en 72,6% gelaatsherkenning. Het laagste percentage, met name 66,5% vinden we terug bij de aanvaardbaarheid van spraak- en stemherkenning. De meest acceptabele vorm van toegangscontrole is diegene waar er meest kennis over is. Dit bevestigt heel wat onderzoeksresultaten uit bovenstaande literatuurstudie.

Zo polsen Visser en Hoorweg (2018) naar de algemene aanvaardbaarheid van biometrische technieken voor het bepalen van je identiteit. 56% is (zeer) positief en aanvaardt dit, 31% blijft neutraal en 18% is (zeer) negatief. Wat betreft het gebruik van camera's in de publieke ruimte met gezichtsherkenning antwoordt 64% (zeer) positief, is 24% neutraal en neemt 13% een (zeer) negatieve houding aan. Cehic & Quigley (2005) vinden op basis van onderzoek uit de Verenigde Staten nog een hogere aanvaardbaarheid van de vingerafdruk als legitiem identificatiemiddel. 91% vindt het geven van een vingerafdruk gerechtvaardigd als vorm van toegangscontrole in een hoog beveiligd gebied en 74% zou dit aanwenden in financiële procedures.

Insites Consulting (2016) concludeert dat 52% van de Belgen klaar is om biometrische betaalmethodes te gebruiken, zoals betalen met vingerafdrukherkenning of met een selfie (Mastercard, 2019). In België opteert één op de twee Belgen voor biometrie om toegang te krijgen tot online-accounts, aldus Van Nuffel (2017). Men beschouwt dit als een waardig alternatief voor paswoorden en 6/10 vindt dit veiliger dan paswoorden. De techniek die de voorkeur geniet, betreft de vingerafdruk (59%) in eerste instantie, de irisscan in tweede instantie (47%) en vervolgens de gezichtsherkenning (27%) en stemherkenning (20%) (Van Nuffel, 2017). De percentages in onze survey zijn hoger, niettemin kent de techniek van de vingerafdrukherkenning ook hier de hoogste graad van acceptatie.

Krupp, Rathgeb & Busch (2013) gaan ook in op de sociale acceptatie van biometrische technieken. De grootste acceptatie wordt gevonden voor de vingerafdrukherkenning, tevens de meest gekende vorm van technologie. Naast de kennis over de technologie speelt volgens Krupp et al. (2013) het gebruik ervan evenzeer een fundamentele rol in het acceptatieproces: hoe meer een technologie wordt gebruikt, hoe meer dit sociaal wordt aanvaard. El-Abed et al. (2012) bevestigen het belang van kennis én het gebruik van biometrische technieken in de aanvaarding ervan (El-Abed et al., 2012).

Hoewel technieken zoals face, speaker en voice recognition gekend zijn, worden deze technieken beduidend minder aanvaard in het onderzoek van Krupp et al. (2013). 25% aanvaardt dit zelfs helemaal niet, wat overeenstemt met onze onderzoeksresultaten. Namelijk 33,5% aanvaardt geen spraak- en stemherkenning en 27,4% aanvaardt geen gelaatsherkenning. De respondenten uit het onderzoek van Krupp et al. (2013) verklaren hun niet-aanvaardbaarheid door het feit dat dit te persoonlijk is, te intiem is en dit wordt zelfs als beangstigend omschreven.

Tot slot wordt in het onderzoek van het Ada Lovelace institute (2019) gepeild naar de biometrische vorm (vingerafdrukken, iris/eye scanning, voice recognition, facial recognition) waar men zich meest comfortabel bij voelt. Als er ingezoomd wordt op het antwoord "*I am not comfortable with using this method of identification*" vinden we de laagste score bij vingerafdrukken. Namelijk 13% duidt dit antwoord aan. Bijna 40% duidt dit antwoord aan bij 'voice recognition' en 32% vinkt dit aan bij facial recognition. Dit bevestigt de onderzoeksresultaten over de aanvaarding van vingerafdrukken.

6.3 Waar wens ik vingerafdrukken te geven?

De bereidheid tot het geven van een vingerafdruk als vorm van toegangscontrole is het hoogst voor wat betreft het ontgrendelen van de smartphone. Dit wordt verklaard door het feit dat dit een zeer courante praktijk is, wat de idee bevestigt van 'hoe meer het in gebruik is genomen, hoe groter de aanvaardbaarheid' (o.a. El-Abed et al., 2012; Krupp, Rathgeb & Busch, 2013) Dit wordt bevestigd in de literatuurstudie waarbij het gebruik van biometrische gegevens stijgt in allerhande sectoren. De tweede plaats die een hoge mate van aanvaardbaarheid krijgt, is het bedrijf waarin men werkt. De luchthaven is de derde toelaatbare sector – bijna 70% is bereid - een sector waarin zowel vingerafdrukken als handpalmscanners frequent gebruikt worden[10].

Ongeveer 64% van de respondenten is bereid om via vingerafdrukken toegang te krijgen tot financiële instellingen. Deze bereidwilligheid wordt in ander onderzoek bevestigd. Zo concludeert Insites Consulting (2016) dat 52% van de Belgen klaar is om biometrische betaalmethodes te gebruiken en één op de twee Belgen opteert voor biometrie om toegang te krijgen tot online-accounts, aldus Van Nuffel (2017). Van de verschillende biometrische technieken die worden voorgelegd, kennen de vingerafdrukken de hoogste mate van aanvaardbaarheid.

Het Global Market Insights report (2017) berekent dat de bank en financiële wereld sterke afnemers zijn van biometrische toepassingen. Febelin (2016) verwijst naar de banken als grootste vragende partij om biometrische gegevens te gebruiken. Een cruciale factor is het vertrouwen van de burger in de banksector. Global Market Insights voorspelt dat er veel groeimarge is en de bank – en financiële wereld dit nog meer zal implementeren in de toekomst.

De plaatsen waar er minst bereidheid is om via de vingerafdruk toegang toe te krijgen, betreffen het shoppingcentrum, de openbare parking en het openbaar vervoer zoals de trein, tram, metro en bus.

[10] Supra.

6.4 Aanwending van technologie in specifieke sectoren

Er is een verband tussen acceptatie en vertrouwen (Koops & Vedder, 2001; Dinev et al., 2005). Respondenten die publieke autoriteiten vertrouwen, zijn sneller geneigd om het gebruik van technologie door deze autoriteiten te aanvaarden (Vermeersch & De Pauw, 2017; Van den Broek et al., 2017). Het type actor is daarenboven belangrijk, zo blijkt er meer aanvaarding te zijn als het publieke sectoren betreft in vergelijking met private sectoren. Uit onderzoek naar het vertrouwen in de politie, blijkt dat het vertrouwen vrij hoog is bij burgers ten aanzien van de politie (Verwee, 2012).

Mitrou, Drogkaris & Leventakis (2018) geven in hun onderzoek aan dat respondenten de voorkeur geven aan CCTV camera's die toegankelijk zijn voor Law Enforcement Agencies. Biesiot et al. (2018) bevestigen dit in Nederlands onderzoek waarbij de opinie over sensing aan de burgers wordt gevraagd. Dit wordt bevraagd in relatie tot het gebruik van sensortoepassingen door de politie. Verschillende scenario's worden voorgelegd. In het mobiele scenario wordt toezicht uitgeoefend door middel van vaste of mobiele camera's en staat de vraag centraal wie dit mag aanwenden. Het feit dat de politie deze sensortechnologie aanwendt, wordt als positief ervaren, niettemin worden hier een aantal kritische randvoorwaarden aan verbonden zoals een goede beveiliging van camera's, een duidelijk doel, effectieve opvolging van de misdaad als er een misdaad gebeurt… Er is minder enthousiasme bij private bewakingsbedrijven die dergelijke technologie gebruiken omdat zij minder gebonden zijn aan regels dan de politie, aldus Snijders et al. (2018).

Onze onderzoeksresultaten bevestigen in grote mate bovenstaande bevindingen. Camera's kunnen volgens 81,4% van de respondenten aangewend worden door de politie. Als dit percentage vergeleken wordt met het percentage waarbij burgers aangeven dat private bewakingsbedrijven en/of de brandweer camera's mogen gebruiken, is dit lager, namelijk 72,2%. Het gebruik van camera's wordt meer getolereerd door politie in vergelijking met andere personen of organisaties. We stellen dit niet alleen vast als we politie vergelijken met private bewakingsbedrijven en brandweer maar dit geldt evenzeer voor winkels en shoppingcentra, openbare vervoersmaatschappijen, medische diensten en onderwijsinstellingen. Het onderzoek van Snijders et al. (2018) bevraagt daarnaast of slimme camera's kunnen aangewend worden door veiligheidspersoneel van de Nationale Spoorwegen (NS). Men tolereert dit ten aanzien van het veiligheidspersoneel, wat ook strookt met ons aantal respondenten dat stelt dat openbare vervoersmaatschappijen gebruik mogen maken van camera's (namelijk 67%). Een lagere tolerantie vinden we zowel in het Belgisch als Nederlands onderzoek bij burgers die camera's mogen aanwenden.

Ook andere biometrische technieken worden getolereerd door burgers als de politie deze aanwendt. Vingerafdrukken kunnen volgens 80,1% van de respondenten gebruikt worden door de politie. Aangaande de andere technieken zijn dit beduidend lagere percentages: bij gelaatsherkenning is dit 59,2%, bij irisscans is dit 52,6% en bij spraak/stemherkenning is dit 48%.

Het tweede scenario uit het Nederlands onderzoek bevraagt het gebruik van automatische gezichtsherkenning. Over het gebruik hiervan door de politie, rijzen enkele kritische vragen zoals de bezorgdheid dat men ten onrechte wordt gevolgd, dat er geen toestemming wordt gegeven om iets te filmen… Op de vraag of de automatische gezichtsherkenning kan gebruikt worden in de publieke ruimte, wordt negatief gereageerd. Deze negatieve reactie weerspiegelt zich bovendien in onze onderzoeksresultaten waarbij gelaatsherkenning door minder dan 1/5de van de respondenten wordt getolereerd in publieke ruimtes zoals winkels en shoppingcentra, openbare vervoersmaatschappijen en onderwijsinstellingen. Het onderzoek van Visser en Hoorweg (2018) concludeert echter dat 74% positief staat ten opzichte van de inzet van camera's in de publieke ruimte om afwijkend gedrag te detecteren (cfr. Framing). De inzet van publieke camera's met gezichtsherkenning wordt door 60% (zeer) positief bejegend. De Belgische Smart City Meter (2018) bevraagt evenzeer het draagvlak voor camera's in functie van veiligheid waarbij 56,5% akkoord gaat met het gebruik van gezichtsherkenning in winkelstraten. Dit cijfer is beduidend hoger ten opzichte van onze onderzoeksresultaten.

59,2% van onze respondenten duidt aan dat de politie de techniek van gezichtsherkenning mag gebruiken. Indien we deze resultaten van de politie vergelijken met de overige sectoren, merken we beduidend lagere percentages op bij de andere sectoren. Volgens 35,1% kunnen medische diensten hiervan gebruik maken en een kleine 30% stelt dat dit kan toegepast worden door private bewakingsbedrijven of brandweer. Een vijfde van de respondenten stelt dat deze techniek door onderwijsinstellingen of openbare vervoersmaatschappijen kan gebruikt worden.

Op basis van een recente survey in de UK (Ada Lovelace institute, 2019) concluderen we dat de bereidheid om facial recognition te aanvaarden hoger is als dit een publiek voordeel oplevert. Zo acht 70% van de respondenten facial recognition toelaatbaar door de politie bij crimineel onderzoek en vindt 50% dit goed om smartphones en systemen te 'unlocken' (50%) in de veronderstelling dat er afdoende beveiliging is. Als we

het percentage van de politie in de UK bekijken ten opzichte van België merken we een verschil op van 10%, niettemin is dit een duidelijk positief antwoord. De reden hiertoe is dat de aanwending van facial recognition door de politie de veiligheid in de samenleving ten goede komt. Er worden opvallend lage percentages van acceptatie vastgesteld in de UK ten aanzien van supermarkten, scholen, bedrijven… Zo is 67% "*uncomfortable*" met het gebruik van facial recognition in scholen en voelt 61% zich niet comfortabel met het gebruik hiervan op publiek transport. In onze survey acht zo'n 20% van de respondenten het toelaatbaar dat onderwijsinstellingen (22,1%), openbare vervoersmaatschappijen (19,3%) en winkels en shoppingcentra (16,6%) gelaatsherkenning mogen gebruiken. Beide onderzoeken tonen een gelijkaardige trend aan, namelijk dat de aanvaardbaarheid van het gebruik van gelaatsherkenning bij politie groot is en deze bij openbare vervoersmaatschappijen, onderwijsinstellingen en commerciële aangelegenheden veel lager is.

Bedrijven die facial recognition gebruiken voor commerciële voordelen, worden in veel mindere mate aanvaard. Zo voelt 77% zich oncomfortabel met de idee dat facial recognition gebruikt wordt door winkels om consumenten te 'tracken' en voelt 76% zich niet comfortabel dat deze technologie wordt aangewend voor Human Resources doeleinden, zoals rekrutering. Het doel waarom facial recognition gebruikt wordt, is dus van groot belang. Het publieke belang – zoals het verhogen van de veiligheid of de bescherming – is veel fundamenteler voor de burger in het acceptatieproces van facial recognition dan het commerciële belang (Ada Lovelace institute, 2019).

Het is tot slot opvallend dat burgers stellen dat sociale media het minst gebruik mag maken van dergelijke technologieën zoals camera's, vingerafdrukken, irisscans, spraak/stemherkenning, gelaatsherkenning… en dat de sector 'sociale media' het hoogst scoort bij het antwoord 'geen van deze technieken', wat impliceert dat 61% van de respondenten stelt dat de sociale media geen van deze technieken mag aanwenden.

6.5 Verband tussen aanvaarding en bereidheid om privacy in te ruilen met veiligheid

Een kleine meerderheid van de respondenten uit onze survey is bereid om privacy in te ruilen voor meer veiligheid. Met name is 57,5% in meer of mindere mate hiertoe bereid en is 42,5% in (helemaal) niet bereid om privacy te ruilen voor meer veiligheid. Het kruisen van de aanvaarbaarheid van biometrische technieken met deze 'ruilvraag' levert significante verbanden. Personen die niet bereid zijn om privacy in te ruilen voor meer veiligheid, aanvaarden minder het gebruik van vingerafdrukken als vorm van toegangscontrole. Deze zelfde tendens geldt voor alle biometrische vormen die bevraagd worden. Dit betekent dat de respondenten die vingerafdrukken, irisscans, spraak/stem-, gelaats- en handpalmherkenning aanvaarden meer bereid zijn om privacy in te ruilen voor meer veiligheid. Personen die biometrische technieken niet aanvaarden, zijn minder geneigd om privacy in te ruilen voor meer veiligheid.

Vermeersch & De Pauw (2017) bevestigen dit onderzoeksresultaat: hoe meer zorgen men zich maakt inzake privacy, hoe minder men geneigd is om het gebruik van technologie te aanvaarden. De respondenten uit hun privacy frame zijn veel minder geneigd om technologie te accepteren. De privacy awareness beïnvloedt de aanvaardbaarheidsniveau 's op een negatieve manier. Een hoog niveau van veiligheidszorg correspondeert positief met het aanvaardbaarheidsniveau. Als mensen zich dus veel zorgen maken over veiligheid, zullen zij de inzet van technologie sneller aanvaarden (Van den Broek et al., 2017). In onze survey zijn de respondenten die geen biometrie aanvaarden, diegenen die niet of minder bereid zijn om privacy in te ruilen voor veiligheid, en wellicht een veel hogere privacy awareness hebben.

Europees SurPRISE onderzoek (Pavone et al., 2015) toont tot slot aan dat burgers meer veiligheid én meer privacy wensen. Het betreft dus niet zozeer een 'of-of' verhaal maar een 'en-en' verhaal. Als SOST's worden geïmplementeerd moet dit op een transparante manier gebeuren, onder legale strikte condities alvorens deze aanvaard worden en als effectief gepercipieerd worden. Tot deze conclusie komen Mitrou et al. (2017) evenzeer. Zij spreken over een Griekse paradox waarbij de Grieken zowel veiligheid als privacy cruciaal vinden en deze begrippen elkaar niet noodzakelijkerwijs uitsluiten. Van den Broek et al. (2017) bevestigen de resultaten van het SurPRISe project alsook deze van het PRISM project waarin veiligheid en privacy niet noodzakelijk aan elkaar gelinkt zijn en burgers beide willen.

6.6 Leeftijd speelt een cruciale rol

De leeftijd speelt in deze biometrie survey een belangrijke rol. Als de antwoorden van de respondenten gekruist worden met de achtergrondvariabelen merken we op dat de leeftijd frequent een significant effect genereert.

De bevraagden tussen 18 en 34 jaar hebben meer kennis over de biometrische technieken en weten beter wat deze technieken inhouden ten opzichte van andere leeftijdscategorieën. Dezelfde leeftijdscategorie is bovendien sterk vertegenwoordigd bij de respondenten die minder bereid zijn om via vingerafdrukken toegang te krijgen tot 'het bedrijf waar anderen werken', 'sportclub', 'in een voetbalstadion of dergelijke', 'muziekfestival' en 'onderwijsinstellingen' in vergelijking met de + 34-jarigen. De niet-bereidwilligheid is nog hoger bij 18 tot 34-jarigen voor wat betreft het geven van vingerafdrukken als toegangscontrole tot het 'openbaar vervoer zoals de trein, tram, metro en bus', 'shoppingcentrum' en 'openbare parking'.

Tot slot valt de jongste leeftijdscategorie op bij de bereidheid om privacy in te ruilen voor meer veiligheid. De 18 tot 34-jarigen duiden vaker 'niet bereid' aan en de 55-plussers zijn hiertoe vaker 'wel bereid'.

7 Conclusies en aanbevelingen

De technologische ontwikkelingen gaan bijzonder snel en het gebruik van heel wat digitale technieken is een evidentie geworden. Dit geldt evenzeer voor de aanwending van biometrische technieken. Dergelijke technieken zorgen voor gebruiksgemak, zoals het ontgrendelen van de smartphone gaat sneller door middel van vingerafdrukken, iris- of gezichtsherkenning in plaats van een traditioneel paswoord te geven. Biometrische technieken worden ook aangewend als toegangscontrole waarbij vaak twee doelen tegelijkertijd gediend worden, namelijk efficiënte en snelle toegangscontrole alsook de garantie op veilige toegang tot het gebouw. De aanwending van biometrische technieken steeg sterk na de aanslagen van 11 september 2001 waarin men paal en perk wou stellen aan identiteitsfraude en andere vormen van criminaliteit. Biometrische gegevens zijn bovendien vaak uniek en erg handig want men heeft ze altijd bij, wat niet het geval is bij een toegangsbadge.

Bij de aanwending van biometrische technieken moet men rekening houden met het wetgevend kader. De wetgevende bepalingen van biometrische gegevens (voor zowel het opvragen van de persoonsgegevens als de verwerking ervan) worden op internationaal en nationaal niveau geregeld. Op internationaal niveau is de General Data Protection Regulation van toepassing, alsook de wetgeving van de Council of Europe en het Europees Verdrag tot bescherming van de Mens en de fundamentele vrijheden. Op nationaal niveau geldt de Belgische gegevensbeschermingswet en enkele Grondwetsartikelen.

De groeiende aanwending van biometrische technieken leidt tot allerhande discussies tussen voor- en tegenstanders. Terwijl verhoogde efficiëntie en veiligheid als voordelen worden benoemd, benadrukken de tegenstanders het belang van privacy. Bij zowel het opvragen van de persoonsgegevens als de verwerking ervan worden principes zoals wenselijkheid en proportionaliteit door critici in de verf gezet: is het wenselijk dat burgers door middel van vingerafdrukken zich identificeren? Is het in proportie met het beoogde doel (cfr. veiligheid, eenvoudige toegang…)? Quid de opslag van gegevens? Wat gebeurt er met de gegevens? In welke databank worden deze gegevens opgeslagen en wie heeft er toegang tot deze databank? En wat als deze gegevens gestolen of 'gehackt' worden?

De implementatie van nieuwe technologieën is noodzakelijk om zich als samenleving tegen ieder denkbaar risico te beschermen. Het gebruik van biometrie wordt omwille van die reden als legitiem beschouwd (Vermeersch & De Pauw, 2017). De neiging om alles te gaan controleren wordt echter ook aan kritiek onderworpen wat volgens sceptici leidt tot een overprotectie waarin een cultuur van angst domineert. Als resultaat van een toenemend gebruik van nieuwe technologie door private en publieke organisaties in een zone van grijze wetten is er een 'silent erosion of privacy'.

Niettemin stellen we een stijgend gebruik van deze technologieën vast. Meer en meer duiken stemmen op die het belang onderschrijven van deze nieuwe surveillancevormen, aldus Vermeersch & De Pauw (2017). Omwille van die reden wordt meer en meer onderzoek gevoerd naar het draagvlak en de aanvaardbaarheid van deze technologieën. Dit is evenzeer de bedoeling van onze survey. Een representatieve steekproef wordt getrokken in België en 1000 burgers worden bevraagd omtrent de aanwending van biometrische technieken. De volgende onderzoeksvragen staan in onze survey centraal: Kent de burger biometrie? Wat denkt de burger over biometrie? Is hoeverre is er een acceptatie van biometrie en hoe groot is deze acceptatie? Wat vindt men over vingerafdrukherkenning als vorm van toegangscontrole? Op welke plaatsen kan vingerafdrukherkenning worden toegepast? Welke actoren mogen welke vormen van biometrie gebruiken. En quid privacy? Is men bereid privacy in te ruilen voor meer veiligheid?

Vias institute bestudeert de voorhanden zijnde literatuur inzake de burgers opinie over biometrie en bevraagt de burger aangaande de aanwending van biometrie. Op basis van deze resultaten worden enkele belangrijke conclusies getrokken.

De kennis die men heeft varieert naargelang de techniek. De meest gekende techniek is deze van de vingerafdrukken: maar liefst 85% kent vingerafdrukken en weet wat het inhoudt. Dit wordt bevestigd door middel van buitenlands onderzoek (o.a. Krupp, Rathgeb & Busch, 2013; Ada Lovelace institute, 2019). De tweede meest gekende techniek betreft deze van gelaatsherkenning (68,2% kent dit), in derde instantie betreft dit spraak- en stemherkenning (66,7% kent dit). De minst gekende techniek is deze van de handafdrukherkenning, namelijk kent 30% dit niet.

Als we bij deze vraag kijken naar de achtergrondvariabelen, stellen we vast dat de respondenten tussen 18 en 34 jaar vaak meer kennis hebben over deze biometrische technieken. Zij weten meer wat deze technieken inhouden in vergelijking met andere leeftijdscategorieën.

Er is een hoog maatschappelijk draagvlak voor biometrische toepassingen, zo aanvaardt 87% van de respondenten het gebruik van vingerafdrukken als een vorm van toegangscontrole. In onze survey blijkt dus dat de aanvaardbaarheid het hoogst is voor de vingerafdrukherkenning, tevens de meest gekende techniek. De kennis over een bepaalde techniek is fundamenteel voor wat betreft de aanvaardbaarheid ervan. Hoe meer men vertrouwd is met een bepaalde techniek, hoe meer deze wordt aanvaard (Koops & Vedder, 2001; Dinev et al., 2005). De aanvaarding van de irisherkenning komt op de tweede plaats, handafdrukherkenning op de derde plaats en de vierde plaats is voor de techniek van gelaatsherkenning. De hoogste niet-aanvaardbaarheidsscores vinden we terug bij spraak- en stemherkenning. Het is verder opvallend dat voornamelijk 55-plussers vingerafdruk- en irisherkenning meer aanvaarden als vorm van toegangscontrole.

Indien men een technologie wenst te implementeren zijn kennis en communicatie cruciaal. Bij de inzet van technologie is steeds een discussie nodig over "*het hoe, wat, waar, wanneer en vooral ook waarom*" (Snijders et al. 2019) bij de burger. Als er geen kennis is, wordt de burger gelimiteerd in de deelname aan het publieke debat over de inzet van biometrische technieken in de samenleving. Ada Lovelace Institute (2019) poneert dat publiek engagement en educatie de democratische basis van deze nieuwe technologieën versterkt. In dit onderzoek geeft de helft van de respondenten aan dat zij de mogelijkheid moeten krijgen om te kiezen of toestemming te geven indien facial recognition wordt gebruikt. Dit blijkt vaak in strijd is met juridische nationale kaders.

De hoogste bereidwilligheid om de vingerafdruk te gebruiken als vorm van toegangscontrole vinden we terug voor het ontgrendelen van de smartphone, namelijk 81,4% is hiertoe bereid. Vervolgens wordt het bedrijf waarin men werkt aangeduid door 71,1% en in derde instantie de luchthaven (69,3%). De reden waarom het ontgrendelen van de smartphone hoog scoort, heeft wellicht te maken met de frequente toepassing hiervan. Dit is immers een zeer courante praktijk. De bereidheid tot het geven van een vingerafdruk is lager bij de jongste leeftijdsgroepen en is het hoogst bij de respondenten die ouder zijn dan 55 jaar.

De politie mag volgens de respondenten het vaakst technologie evenals biometrische technieken aanwenden. 81,4% geeft aan dat de politie camera's mag gebruiken, 80,1% vindt dat politie vingerafdrukken mag gebruiken, 59,2% stelt dat dit het geval is voor gelaatsherkenning en volgens 52,6% mag de politie irisscans gebruiken. Dit wordt verklaard door het vertrouwen dat er is in de politie. Er is een verband tussen acceptatie en vertrouwen en onderzoek toont aan dat het vertrouwen in de politie vrij hoog is (Verwee, 2012). Respondenten die publieke autoriteiten vertrouwen zijn sneller geneigd om het gebruik van de technologie door deze autoriteiten te aanvaarden (Vermeersch & De Pauw, 2017; van den Broek et al., 2017; Mitrou et al., 2018; Snijders et al. 2019; Ada Lovelace institute, 2019). De burgers zijn minder enthousiast wanneer private bedrijven dergelijke technieken aanwenden. Ze stellen zich meer vragen omtrent de toepasbaarheid, ethiek, privacy, verzameling van data…

De meest sceptische houding voor het aanwenden van de technologie vinden we bij de sociale media. 61% stelt dat de sociale media geen enkele van deze technieken mag aanwenden.

De acceptatie van de aanwending van biometrische technieken is opvallend veel hoger bij de politie dan bij andere sectoren. Dit wordt door ons vastgesteld en veelvuldig bevestigd in ander onderzoek. Het vertrouwen dat de politie geniet als publieke instelling wordt als verklaring opgeworpen. Het doel waarom biometrische technieken gebruikt worden, is evenzeer van groot belang. Het publieke belang – zoals het verhogen van de veiligheid of de bescherming – is veel fundamenteler voor de burger in het acceptatieproces van facial recognition dan het commerciële belang (Ada Lovelace institute, 2019). De makers en gebruikers van deze technologie "*need to consider these trade-offs, as well as to engage the wider public understanding in how to navigate them*" (Ada Lovelace Institute, 2019). Bij de implementatie van dergelijke technologieën is het cruciaal om te reflecteren of dit de publieke verwachtingen en normen reflecteert. Het bestuderen van de publieke opinie gebeurt weinig en dient aangemoedigd te worden opdat een debat ten gronde kan georganiseerd worden. Het meten van publieke opinie mag geen doel op zich zijn maar is een maatstaf om te zien of dit hetgeen is wat het publiek wil en waarom men dit al dan niet wenst.

De acceptatie van de aanwending van bepaalde technieken door politie is echter niet ongelimiteerd. Zo zijn garanties nodig, beveiliging en vindt men een regelgeving noodzakelijk. De publieke acceptatie van een biometrische techniek hangt vaak af van de case waarin deze gebruikt wordt (Snijders et al. 2019); zo is het mogelijk dat burgers aanvaarden dat bodycams kunnen gebruikt worden door de politie maar niet door de pizzakoerier. De context en de omstandigheden waarin deze geïmplementeerd worden, zijn cruciale factoren in dit aanvaardingsproces "*each application of technology requires its own public engagement process, trials and evidence base*" (Ada Lovelace Institute, 2019). Allerhande mogelijke applicaties van technologieën kunnen hierbij overschouwd worden: wat zijn voor- en nadelen, knelpunten, bekommernissen… Het begrijpen van de publieke attitudes - bijvoorbeeld door middel van het voorleggen van specifieke scenario's - is hierbij cruciaal.

Zo weet men niet alleen wat de technologie kan en doet maar ook wat de aanwending van de technologie in een specifieke context impliceert.

Er is een belangrijke rol weggelegd voor de overheid. De overheid kan de burger educeren, dialoog stimuleren én dient ook te reguleren. Het reguleren kan door algemene juridische kaders maar ook door het opleggen van specifieke regels aan sectoren (publieke sectoren en private sectoren). In het Verenigd Koninkrijk zijn de burgers vragende partij voor een vrijwillige 'pauze' van de bedrijven die facial recognition technologie verkopen aan politie of scholen. Eerst dient er een publieke consultatie hierover plaats te vinden waarbij er de nodige aandacht is voor ethische en verantwoordelijke regulatie voor de aanwending van deze technologie. Ada Lovelace Institute (2019) wenst publieke consultatie te stimuleren door een "*Citizens' Biometric Council, a citizen's assembly supported by the Information Commissioner's Office*".

Critici halen vaak het argument van privacy als reden aan om biometrische technieken niet te gebruiken als verificatie of toegangscontrole. In onze survey is een kleine meerderheid van de respondenten, namelijk 57,5%, bereid om privacy in te ruilen voor meer veiligheid. De extreme antwoorden scoren lager: men is dus 'eerder wel bereid' of 'eerder niet bereid' om privacy in te ruilen voor meer veiligheid. Als we deze resultaten kruisen met de vraag naar aanvaardbaarheid zien we dat de respondenten die biometrische technieken aanvaarden, meer bereid zijn om privacy in te ruilen voor veiligheid. Dit impliceert dat degene die de techniek niet aanvaarden doorgaans minder (of niet) bereid zijn om privacy in te ruilen voor veiligheid. Aangaande privacy en veiligheid is het tot slot belangrijk dat onderzoek aangeeft dat dit een 'en-en'- in plaats van een 'of-of'-verhaal is waarbij burgers privacy én veiligheid willen. Dit wordt bevestigd in het Europese SuRPISE onderzoek. De resultaten van Pavone et al. (2015) tonen aan dat burgers zowel meer veiligheid als meer privacy wensen (cfr. en-en-verhaal) en dat Surveillance Oriented Security Technologies (SOST's) op een transparante manier moeten geïmplementeerd worden onder strikte legale condities om te worden aanvaard en als effectief te worden gepercipieerd.

We concluderen tot slot met een aantal 'spelregels' voor surveillance met sensoren, komende vanuit de burger. SurPRISE vroeg namelijk aan burgers welke de criteria en argumenten zijn omtrent het gebruik van sensortechnologie. Deze criteria en argumenten kennen een internationaal karakter. In eerste instantie moet het gebruik van sensortechnologie onder een Europees raamwerk van regels vallen, onder controle van een Europese instantie. De uitvoering moet ingebed zijn in transparante procedures voor gegevensbescherming en aansprakelijkheid, is in handen van overheidsinstellingen en wordt alleen voor publieke doelen ingezet. Als private partijen betrokken zijn, moet dit aan strikte regulering worden onderworpen. De aanwending van sensortechnologie impliceert dat de voordelen opwegen ten opzichte van de nadelen, in vergelijking met andere (niet-) technische alternatieven die minder inbreuken veroorzaken. De uitvoering ervan is te reguleren via instemming van de betrokkenen (cfr. opt-in approach), zij hebben toegang tot hun eigen data en kunnen deze aanpassen of verwijderen. Het moet gericht zijn op minder gevoelige data en ruimtes, volgens criteria en doelen die publiekelijk bekend zijn. De inzet van sensortechnologie is gebonden aan specifieke doelen, tijden en plaatsen en op basis van privacy-by-design ontworpen. Tot slot worden "*deze in combinatie met niet-technische maatregelen en sociale strategieën ingezet die zich richten op de sociale en economische oorzaken van onveiligheid*" (Pavone et al., 2015).

Referenties

Ada Lovelace institute (2019). *Beyond face value: public attitudes to facial recognition technology*. Retrieved from https://www.adalovelaceinstitute.org/beyond-face-value-public-attitudes-to-facial-recognition-technology/ [10/10/2019].

Assens, M. (2019). *History of Voice Recognition*. Retrieved from http://www.happyscribe.co/blog/history-voice-recognition/ [25/03/2019].

Augustyn, A., Bauer, P., Duignan, B., Eldridge, A., Gregersen, E., Luebering, J.E., McKenna, A., Petruzzello, M., Rafferty, J.P., Ray, M., Rogers, K., Tikkanen, A., Wallenfeldt, J., Zeidan, A. & Zelazko, A. (2019). *Alphonse Bertillon*. Retrieved from https://www.britannica.com/biography/Alphonse-Bertillon [25/03/2019].

Aussems, M. (2018). *Ogen, duimen en GDPR: breekt biometrie door bij bedrijven?.* Retrieved from https://www.smartbiz.be/achtergrond/173793/ogen-duimen-en-gdpr-breekt-biometrie-door-bij-bedrijven/ [26/03/2019].

BBC (2017). *Daarom lanceert dit park wc-rollen met gezichtsherkenning*. Retrieved from https://www.nieuwsblad.be/cnt/dmf20170320_02789404 [20/03/2017].

Beirne, P. (1987). *Adolphe Quetelet and the Origins of Positivist Criminology*. 92: 1140-1169.

Belga (2018). Privacycommissie is tegen vingerafdrukken op ID-kaart. *Het Laatste Nieuws*.

Belga (2018). Liga voor Mensenrechten: Vingerafdrukken op identiteitskaart in strijd met recht op privacy. *De Morgen*.

Belga (2019). Experts maken brandhout van vingerafdrukken op identiteitskaarten. *De Gazet Van Antwerpen*.

Beveiligingsnieuws (2019). *Europese Commissie wil strikte regels voor gezichtsherkenning*. Retrieved from https://beveiligingnieuws.nl/nieuws/europese-commissie-wil-strikte-regels-voor-gezichtsherkenning?utm_source=dlvr.it&utm_medium=twitter [27/8/2019].

Biesiot, M., de Bakker, E., Jacquemard, T., van Est, R. (2018). *Hoe kijken burgers naar het gebruik van sensordata voor leefbaarheid en veiligheid?* Den Haag: Rathenau Instituut.

BiometricNews (N.d.). *BiometricNews.net*. Retrieved from http://biometricnews.net/project/signature-recognition/.

Broerders, A.P.A. & Muller, E. (2008). *Forensische Wetenschap.* Wolters Kluwer.

Bruggeman, F. (2018). *Gezichtsherkenning gaat erg ver in China: de weg naar een digitaal totalitarisme?* Retrieved from https://www.vrt.be/vrtnws/nl/2018/11/28/gezichtsherkenning-china/ [28/11/2018].

Budak, J., Rajh, E. & Rechner, V. (2017). Citizens' privacy concerns. Does national culture matter? In: Friedewald, M, Burgess, J.P., Cas, J., Bennanova, R., Peissl, W. (2017). *Surveillance, Privacy and Security – Citizens' Perspectives*. London: Routledge, pp. 36-51.

Cehic M. & Quigley M. (2018). *Ethical Issues Associated with Biometric Technologies*. Retrieved from http://www.irma-international.org/viewtitle/32657/ [02/04/2019].

Chaudhari, R. D., Pawar, A.A. & Deore, R.S. (2013). *The historical development of biometric authentication techniques: A recent overview*. 2: 3921-3928.

Datanews (2019). *Facebook zet gezichtsherkenning standaard uit voor iedereen*. Retrieved from https://datanews.knack.be/ict/nieuws/facebook-zet-gezichtsherkenning-standaard-uit-voor-iedereen/article-news-1505159.html [04/09/2019].

De financiële begrippenlijst (2017). *De financiële begrippenlijst*. Retrieved from https://www.dfbonline.nl/begrip/21588/ [25/03/2019].

De Geest, C. (2013). *Vingerafdrukken op de schoolbanken*. Retrieved from http://www.dewereldmorgen.be/artikels/2013/05/22/vingerafdrukken-op-de-schoolbanken [26/03/2019].

Debeuckelaere, W. (2008). *Advies uit eigen beweging over het verwerken van biometrische gegevens in het raam van authenticatie van personen Commissie voor de bescherming van persoonlijke levenssfeer: 22*.

De Pauw, E. & Vermeersch, H. (2015). Politie, surveillantie en technologie. Wie legt de kaarten in 2025? In: Ponsaers, P., Bruggeman, W., Easton, M. & Lemaitre, A. (Eds.). *De toekomstpolitie. Triggers voor een voldragen debat*. Antwerpen: Maklu. Pp. 165- 186.

Dhairya, P. (2018). *Facial recognition systems*. Retrieved from https://medium.com/coinmonks/from-the-rand-tablet-to-differentiating-identical-twins-aa4ba6031bb0 [23/04/2019].

Deurplus (2019). *Toegangscontrole gezichtsherkenning – Comfortabel zonder kaart*. Retrieved from https://www.deurplus.com/zakelijk/toegangscontrole/gezichtsherkenning/ [04/2019].

Dinev, T., Masssimo, B., Hart, P., Christian, C. & Vincenzo, R. (2005). Internet Users, Privacy Concerns and Attitudes towards Government Surveillance – An Exploratory Study of Cross-Cultural Differences between Italy and the United States. *BLED 2005 Proceedings.* 30.

D'Huys, V. & Witsenburg, P. (2018). *Het grote GDPR handboek*. 103.

Digital trends (2019). Gebruiken we binnenkort ook Touch ID van iPhone om auto te starten. *Het Laatste Nieuws*.

Dobbelaere-Welvaert, M. (2019). *Stop de vingerafdruk*. Retrieved from https://stopvingerafdruk.be/onze-missie/ [26/03/2019].

Eknoyan, G. (2007). *Adolphe Quetelet (1796–1874)—the average man and indices of obesity*. Nephrology Dialysis Transplantation. 23(1): 47-51.

Elgan, M. (2017). *Dit is de duivelse realiteit van gezichtsherkenning*. Retrieved from https://computerworld.nl/markttrends/97734-dit-is-de-duivelse-realiteit-van-gezichtsherkenning.

El-Abed, M., Giot, R., Hemery, B. & Rosenberger, C. (2012). Evaluation of Biometric Systems: A study of Users' Acceptance and Satisfaction. *Inderscience International Journal of Biometrics*, pp. 1-27.

Ensie (2019). *Wat is de betekenis van fysiologisch?.* Retrieved from https://www.ensie.nl/betekenis/fysiologisch [25/03/2019].

Europese Commissie (2016). *Stronger and Smarter Borders in the EU: Commission proposes to establish an Entry-Exit System*.

Europese Commissie (2019). *Identification of applicants (EURODAC)*. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/asy-lum/iden-tification-of-applicants_en [25/03/2019].

Febelfin (2016). *Biometrisch betalen: realiteit of utopie*. Retrieved from https://www.febelfin.be/nl/biometrisch-betalen-realiteit-utopie [26/03/2019].

Federale Overheid Binnenlandse Zaken (2018). *Wijziging van de camerawetgeving: welke veranderingen betekent dit voor jou?*. Retrieved from https://www.besafe.be/nl/nieuws/wijziging-van-de-camerawetgeving-welke-veranderingen-betekent-dit-voor-jou [28/03/2019].

Fundamental rights agency (2018). *Fundamental rights implications of storing biometric data in identity documents and residence cards.* 26.

Gegevensbeschermingsautoriteit (2019). *Het Visa information System (VIS)*. Retrieved from https://www.gegevensbeschermingsautoriteit.be/visa-informatie-systeem [25/03/2019]/.

Gemalto (2019). *Biometrics: authentication and identification*. Retrieved from https://www.gemalto.com/govt/inspired/biometrics [26/03/2019].

Global Market Insights (2017). *Biometric Market Size By Application (Government, Defense Services, Banking and Finance, Consumer Electronics, Healthcare, Transport/Logistics), By Product (AFIS, non-AFIS, Geometry, Signature, Voice, Iris, Face), Industry Analysis Report, Regional Outlook, Application Potential Price Trends, Competitive Market Share & forecast, 2017-2014*).

Gopal, A.V., & Murale, V. (2018) Acceptance of technology by senior citizens. *International Journal of Pure and Applied mathematics*. Retrieved from https://acadpubl.eu/jsi/2018-118-5/articles/5/53.pdf [2018].

Houses Of Parliament (2018). *Biometric Technologies,* 6.

Heukers, M. (2009). *Digitalisering van vingerafdrukken*. Retrieved from van http://www.exo.science.ru.nl/bronnen -/informatica/vinger-afdrukkendigitaliseren.html [21/11/2018].

Imec (2018). *Smart City Meter*. Retrieved from: https://www.imeccityofthings.be/nl/blog/alles-wat-je-moet-weten-over-de-smart-city-meter.

International Criminal Police Organization (N.d.). *INTERPOL's Rules on the Processing of Data*. Retrieved from https://rm.coe.int/interpol-s-rules-on-the-processing-of-data/168073ce01 [21/04/2019].

iStock (2017). *KFC laat je vanaf nu in China betalen door te glimlachen naar een scherm*. *Retrieved from* https://newsmonkey.be [21/04/2019].

Kalyani CH. (2017). Various Biometric Authentication Techniques: A Review. *J Biom Biostat.* 8:5. 371.

Kassin, S., Dror, I., & Kukucka, J. (2013). The forensic confirmation bias: Problems, perspectives, and proposed solutions. *Journal of Applied Research in Memory and Cognition, 2*, 42-52.

Kikel, C. (2019). *A brief history of voice recognition technology. Total voice technologies*. Retrieved from https://www.totalvoicetech.com/a-brief-history-of-voice-recognition-technology/ [25/03/2019].

Kindt, E. J. (2018). Having yes, using no? About the new legal regime for biometric data. *Computer law & security review*, *34* (3), 523-538.

King, R. (2018). *Multiple surveys find acceptance of biometrics by U.S., U.K. consumers mixed*. Retrieved from https://www.biometricupdate.com/201802/multiple-surveys-find-acceptance-of-biometrics-by-u-s-u-k-consumers-mixed.

Koops, E.J. & Vedder (2001). *Opsporing versus privacy: de beleving van burgers*. Den haag: Sdu Uitgvers.

Krupp, A., Rathgeb, C. & Busch, C. (2013). *Social Acceptance of Biometric Technologies in Germany: A Survey*. Retrieved from http://subs.emis.de/LNI/Proceedings/Proceedings212/193.pdf .

Lauryssen, B., Vander Beken, T., Hebberecht, P., Pauwels, L. (2014). *Een crimineel brein: van frenologie tot neurocriminologie*.

Leenders, W. (2007-2008). *Een algemene databank voor vingerafdrukken: veiligheid of privacy?* Vakgroep Strafrecht en Criminologie. Gent, Universiteit Gent: 30 p.

Maguire, M. J. A. T. (2009). *The birth of biometric security*. 25(2): 9-14.

Mastercard (2019). *Biometrisch betalen klaar om in België gecommercialiseerd te worden*. Retrieved from https://newsroom.mastercard.com/eu/nl/press-releases/biometrisch-betalen-klaar-om-in-belgie-gecommercialiseerd-te-worden/ .

Mitrou, L., Drogkaris, P. & Leventakis, G. (2017). Perceptions of videosurveillance in Greece. A Greek paradox beyond the trade-off of security and privacy?. In: Friedewald, M., Burgess, J.P., Cas, J. Bellanova, R. & Peissl, W. (2017). *Surveillance, Privacy and Security – Citizens' Perspectives*. London: Routledge, pp. 123-138.

Miranda, L. (2018). *Thousands of stores will soon use facial recognition, and they won't need your consent.* BuzzFeed News.

Nationaal forensisch onderzoeksbureau (2019). *Vingerafdrukken onderzoek*. Retrieved from https://www.forensischonderzoeksbureau.nl/forensisch-onderzoek/vingerafdruk-ken.html [26/03/2019].

NSTC subcommittee on Biometrics (2006). *Hand Geometry*.

Pavone, V., Santiago, E. & Degli-Esposti, S. (2015). *SurPRISE. Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*. Retrieved from http://surprise-project.eu/wp-content/uploads/2013/10/SurPRISE-D2.2-Draft-Report-on-Key-Factors.pdf .

Peeters, F . (2019). *Gezichtsherkenning vervangt langzaam vingerafdrukscan*. Retrieved from https://www.smartphone.nl/tips/gezichtsherkenning-ios-android/ .

Recogtech (2019). *5 veelvoorkomende biometrische technieken vergeleken*. Retrieved from https://www.recogtech.com/nl/kennisbank/5-veel-voorkomende-biometrische-technieken [26/03/2019].

Recogtech (2019). *Hoe werkt aderpatroonherkenning*. Retrieved from https://www.recogtech.com/nl/kennisbank/aderpatroonherkenning [25/03/2019].

Redactie (2018). *Biometrie: veiliger dan wachtwoorden?*. Retrieved from https://www.kpn.com/zakelijk/blog/biometrie-veiliger-dan-wachtwoor-den.htm [26/03/2019].

Riemen, J. & I. M. Voorhoeven (2015). *Dactyloscopisch ondezoek sporen 15*.

Snijders, D. (2019). *Nieuw onderzoek: sensordata voor veiligheid en leefbaarheid*. Retrieved from: https://www.rathenau.nl/nl/digitale-samenleving/nieuw-onderzoek-sensordata-voor-veiligheid-en-leefbaarheid [05/2019].

Snijders, D., Biesiot, M, Munnichs, G. & van Est, R. (2019). Burgers en sensoren. *Acht spelregels voor de inzet van sensoren voor veiligheid en leefbaarheid*. Den Haag: Rathenau Instituut. Retrieved from: https://www.rathenau.nl/nl/digitale-samenleving/burgers-en-sensoren.

Standaert, K. (2019). 13 op 14 badges gekopieerd met toestel van 40 euro. Dure beveiliging van gebouwen valt in een oogwenk te omzeilen. *Het laatste Nieuws*, 2 mei 2019.

Stellar Business Computing (2018). *Stemherkenning als biometrische verificatie methode populairder*. Retrieved from https://stellarsecuritycomputing.eu/2018/12/18/stemherkenning-populairder-als-biometrische-verificatie-methode/ .

Sustronck, O. (2019). *Vingerscan en gezichtsherkenning, hoe zit dat nu met de GDPR?.* Retrieved from https://gdpr.woltersklu-wer.be/nl/nieuws/vingerscan-en-gezichtsherkenning-hoe-zit-dat-nu-met-de-gdpr/ [26/03/2019].

Tajfel, H. (1974). *Social identity and intergroup behavior*. Information (International Social Science Council), 13(2), 65-93.

Taha, N. (2018). *Facebook zet opnieuw omstreden gezichtsherkenning in*. Retrieved from https://www.hln.be/ihln/internet/facebook-zet-opnieuw-omstreden-gezichtsherkenning-in~ac2881cf/ [02/04/2019]

Thakkar, D. (2018). *Hand geometry recognition biometrics*. Retrieved from https://www.bayometric.com/hand-geometry-recognition-biometrics/ [25/03/2019].

Van den Broek, T., Ooms, M., Friedewald, M., van Lieshout, M. & Rung, S. (2017). The acceptance of new security oriented technologies, a 'framing' experiment. In: Friedewald, M., Burgess, J.M., Cas, J., Bellanova, R. & Peissl, W. (2016). *Surveillance, Privacy and Security – Citizens' Perspectives.* London: Routledge, pp.15-35.

Van Den Boogaerde, V. (2005-2006). *Criminologische relevantie van de irisscan*. Vakgroep Strafrecht en Criminologie. Gent, Universiteit Gent: VIII, 107 p.

Van Eeckhout, S. &. De Beelde, I., (2003). *Beveiliging van gegevensbestanden in Belgische ondernemingen*, Diss. lic. toegepaste economische wetenschappen.

Van Kleef, J. (2018). *Biometrie in militaire operaties*. Retrieved from https://www.militairespectator.nl/sites/default/files/uitgaven/inhoudsopgave/Militaire%20Spectator%201-2018%20Van%20Kleef.pdf .

Van Nuffel, P. (2017). *De helft van de Belgen ziet biometrie wel zitten als alternatief voor wachtwoorden*. Retrieved from https://datanews.knack.be/ict/nieuws/de-helft-van-de-belgen-ziet-biometrie-wel-zitten-als-alternatief-voor-wachtwoorden/article-normal-936227.html .

Varenna (2011). *Geschiedenis van de vingerafdruk*. Retrieved from https://wetenschap.infonu.nl/diversen/67431-geschiedenis-van-de-vingerafdruk.html [25/03/2019].

Veridin (2019). *5 advantages of Biometric Security Systems*. Retrieved from https://www.veridin.com/blog/5-advantages-of-biometric-security-systems/ .

Verwee, I. (2012). *De politierol bekeken door de bril van de burger. Een caleidoscoop van verwachtingen en betekenissen*. Antwerpen: Maklu.

Vermeersch, H. & De Pauw, E. (2017). The acceptance of new security oriented technologies, a 'framing' experiment. In: Friedewald, M., Burgess, J.P., Cas, J., Bellanova, R. & Peissl, W. (2016), *Surveillance, Privacy and Security – Citizens' Perspectives*. London: Routledge, p. 52-70.

Vermeersch, H., Vandenbogaerde, E. & De Pauw, E. (2018). When It Rains in Paris, It Drizzles in Brussels? In: Burgess, P., Reniers, G., Ponnet, K., Hardyns, W. & Smit, W. (Eds.) *Socially Responsible Innovation in Security. Critical Reflections*, 63–82.London: Routledge

Verordening (EU) Van het Europees Parlement en De Raad (2016). Retrieved from https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN [29/3/2019].

Vlavabbs (2019). *Uitstel vingerafdrukken op e-id*. Retrieved from https://www.vlavabbs.be/nieuws/20190406-uitstel-uitrol-vingerafdrukken-op-e-id

Visser, P. & Hoorweg, E. (2018). *Vertrouwen en wantrouwen in de digitale samenleving. Trends in veiligheid 2018*. https://www.capgemini.com/nl-nl/wp-content/uploads/sites/7/2018/06/Trends-in-Veiligheid-2018-report.pdf [04/07/2019].

VRT NWS. (2019). *Broodje betalen? In Sint-Bavo in Gent kan het weldra met de handpalm*. Retrieved from https://www.vrt.be/vrtnws/nl/2019/08/29/broodje-betalen-doen-de-leerlingen-weldra-met-de-handpalm-in-de/ [29/08/2019].

VRT NWS. (2018). *De nieuwe privacywetgeving in 5 vragen: wat verandert er voor u?* Retrieved from: https://www.vrt.be/vrtnws/nl/2018/03/22/de-nieuwe-privacywetgeving-in-5-vragen--wat-verandert-er-voor-u-/ [01/04/2019].

VRT NWS (2019). *Uitrol vingerafdrukken op identiteitskaart loopt mogelijk vertraging op*. Retrieved from VRT News https://www.vrt.be/vrtnws/nl/2019/03/30/uitrol-vingerafdrukken-op-identiteitskaart-loopt-mogelijk-vertra/ [30/03/2019].

VRT NWS (2019). Politie mag geen automatische gezichtsherkenning gebruiken op de luchthaven. Retrieved from VRT News https://www.vrt.be/vrtnws/nl/2019/09/20/politie-mag-geen-automatische-gezichtsherkenning-gebruiken-op-de/ [20/09/2019].

VRT NWS. (2019). *Waarom uw vingerafdruk op uw identiteitskaart gevaarlijk is (en geen enkele crimineel zal stoppen*. Retrieved from https://www.vrt.be/vrtnws/nl/2019/09/29/matthiaas-dobbelaere-opinie/ [30/09/2019].

Zwenne, G. J., & Mommers, L. (2016). De tien belangrijkste veranderingen die de Algemene Verordening Gegevensbescherming gaat brengen. *Tijdschrift voor Compliance*, 2016, 8.

X. (2008). *Schiphol maakt gebruik van irrisscan voor grenspassage flink duurder*. Retrieved from Luchtvaartnieuws.nl.

X. (2016). *Hoe werkt een iris-scanner?*. Retrieved from https://www.portablegear.nl/achtergrond/17764/iris-scanner/ [25/03/2019]

X. (2017). *MasterCard brengt biometrische betaalpas*. Retrieved from https://www.internetkassa.nu/mastercard-brengt-biometrische-betaalpas/ [25/03/2019].

X. (2018). *Face ID: alles wat je wil weten over gezichtsherkenning op de Iphone*. Retrieved from https://www.iculture.nl/uitleg/face-id/ [25/03/2019].

X. (2018). *Grote toename van sectoren die biometrie gebruiken*. Retrieved from https://beveiligingnieuws.nl/nieuws/achtergrond-nieuws/grote-toename-van-sectoren-die-biometrie-gebruiken [25/03/2019].

X. (2019). *Winkelier mag biometrische identificatie niet verplichten*. Retrieved from https://beveiligingnieuws.nl/nieuws/rechtspraak/winkelier-mag-biometrische-identificatie-niet-verplichten?utm_source=dlvr.it&utm_medium=twitter [27/8/2019].

X. (2019). *Betalen met je vingerafdruk. Privacycommissie maakt zich zorgen over plan nieuw plan Carrefour*. Retrieved from Het Nieuwsblad: https://www.nieuwsblad.be/cnt/dmf20191121_04728932 [22/11/2019].

Bijlage

Vragenlijst

1. Welke van onderstaande identificatietechnieken kent u?

	Ken ik en ik weet wat het juist inhoudt	Heb ik al van gehoord maar ik weet niet wat het juist inhoudt	Ken ik niet
Vingerafdrukken	o	o	o
Gelaatsherkenning	o	o	o
Irisherkenning	o	o	o
Handafdrukherkenning	o	o	o
Spraak/stemherkenning	o	o	o

2. Het gebruik van identificatietechnieken bij een toegangscontrole duikt meer en meer op in onze huidige technologische samenleving. Door middel van deze technieken worden lichaamskenmerken van een persoon gemeten of vastgesteld, zoals vingerafdrukken, het gelaat, de iris… en herkend.

   In welk mate vindt u onderstaande identificatietechnieken aanvaardbaar als vorm van toegangscontrole?

	Helemaal niet aanvaardbaar	Niet aanvaardbaar	Eerder niet aanvaardbaar	Eerder wel aanvaardbaar	Wel aanvaardbaar	Helemaal wel aanvaardbaar
Vingerafdrukken (herkent een afdruk van een vinger)	o		o	o	O	o
Gelaatsherkenning (herkent het gelaat)	o		o	o	o	o
Irisherkenning (herkent een iris van het oog)	o		o	o	o	o
Handafdrukherkenning (herkent een handafdruk)	o		o	o	o	o
Spraak/stemherkenning (herkent spraak of stem)	o		o	o	o	o

3. In hoeverre bent u bereid om via uw vingerafdruk toegang te krijgen tot de volgende plaatsen?

	Helemaal niet bereid	Niet bereid	Eerder niet bereid	Eerder wel bereid	Wel bereid	Helemaal wel bereid
In het bedrijf waar ik werk	o		o	o	o	O
In een bedrijf waar anderen werken	o		o	o	o	O
In de sportclub	o		o	o	o	o
In een voetbalstadion of dergelijke	o		o	o	o	o
Op een muziekfestival	o		o	o	o	o
In onderwijsinstellingen	o		o	o	o	o
Op het openbaar vervoer zoals de trein, tram, metro, bus	o		o	o	o	o
Op de luchthaven	o		o	o	o	o
In het shoppingcentrum						
In een openbare parking	o		o	o	o	o
In een private parking	o		o	o	o	o
In een financiële instelling	o		o	o	o	o
In mijn woning						
Om mijn smartphone te ontgrendelen	o		o	o	o	o

4. Duid aan welke van de volgende personen of organisaties volgens gebruik mogen maken van de opgesomde technieken.

	Camera's	Vingerafdrukken	Irisscans	Spraak/stemherkenning	Gelaatsherkenning
Politie	o	o	o	o	o
Brandweer	o	o	o	o	o
Medische diensten	o	o	o	o	o
Openbare vervoersmaatschappijen	o	o	o	o	o
Onderwijsinstellingen	o	o	o	o	o
Private bewakingsbedrijven	o	o	o	o	o
Winkels en shoppingcentra	o	o	o	o	o
Sociale media	o	o	o	o	o
Gewone burgers	o	o	o	o	o

5. In hoeverre bent u bereid om privacy in te ruilen voor meer veiligheid?
    - Helemaal niet bereid
    - Niet bereid
    - Eerder niet bereid
    - Eerder wel bereid
    - Wel bereid
    - Helemaal wel bereid

Vias institute
Haachtsesteenweg 1405, 1130 Brussel · Chaussée de Haecht 1405, 1130 Bruxelles · +32 2 244 15 11 · info@vias.be · www.vias.be