Afstudeerverslag

Forensisch Onderzoek
Hogeschool van Amsterdam

Toegang tot digitale data na overlijden

Student:	Bibi-Jane del Rosario
Studiejaar:	2018-2019
Studentennummer:	500731269
Stage bedrijf:	i-Finish / Digitale Nazorg
Stage begeleider:	Sander van der Meer
Begeleidend docent:	Brenda Hendriks

Voorwoord

Voor u ligt de scriptie ‘toegang tot digitale data na overlijden’. Deze scriptie is opgemaakt door Bibi-Jane del Rosario bij i-Finish en is geschreven in het kader van het afstuderen aan de opleiding Forensisch Onderzoek van de Hogeschool van Amsterdam.

i-Finish is onderdeel van het bedrijf Digitale Nazorg, een kenniscentrum met expertise op het gebied van innovatieve en technische oplossingen bij de digitale nalatenschap, online erfenis en dierbare data. Waar Digitale Nazorg zich sinds 2013 primair richt op het toegankelijk maken van telefoons, computer en overige gegevensdragers na overlijden, houdt i-Finish zich specifiek bezig met het inzichtelijk maken, veiligstellen en opzeggen van on- en offline abonnementen, lidmaatschappen, accounts, clouddiensten en sociale media. In dit verslag wordt voor de leesbaarheid de verzamelnaam i-Finish gebruikt en waar nodig verwezen naar de specifieke diensten.

Ik wil mijn bedrijfsbegeleider Sander van der Meer, mijn begeleidend docent Brenda Hendriks, Marjanka Schaap en Maarten Noordlanden bedanken voor de tijd die zij in mijn onderzoek hebben gestoken en voor de feedback en inzichten die ze mij hebben gegeven.

Amsterdam, juni 2019

Inhoudsopgave:

Samenvatting

Tegenwoordig laat iedereen een digitale erfenis achter op het moment dat ze overlijden. Deze privacygevoelige gegevens kunnen van belang zijn voor de rouwverwerking van de nabestaanden en voor de waarheidsvinding in het kader van de opsporing. Het komt steeds vaker voor dat nabestaanden twijfelen over de doodsoorzaak bij zaken waarbij de politie heeft geconcludeerd dat er waarschijnlijk sprake is van suïcide of een ongeluk. Het is onduidelijk in hoeverre opsporingsambtenaren gebruik kunnen maken van digitale gegevens bij overlijdensgevallen met suïcide als vermoedelijke toedacht. Nabestaanden blijven met veel vragen achter en hebben het belang om digitale gegevens van de overledene in te zien, in de hoop om antwoord te krijgen op hun vragen. Maar digitale gegevens zijn beveiligd door toestelcodes, gebruikersnamen en wachtwoorden. Nabestaanden kunnen dan terecht bij Digitale Nazorg. i-Finish is een dienst van Digitale Nazorg die de mogelijkheid biedt om inhoud van apparatuur en online diensten veilig te stellen. Het is voor commerciële bedrijven echter onduidelijk of hun toegang mogen verschaffen tot digitale gegevens van een overledene.

Het doel van dit onderzoek is om te achterhalen hoe opsporingsambtenaren en nabestaanden zichzelf op een juridisch correcte wijze toegang kunnen verschaffen tot digitale data bij overlijdensgevallen met zelfdoding als vermoedelijke toedracht. Hiervoor is de volgende hoofdvraag opgesteld: *Op welke wijze kunnen opsporingsambtenaren en nabestaanden zichzelf, op een juridische correcte wijze, toegang verschaffen tot digitale data bij overlijdensgevallen met suïcide als vermoedelijke toedracht?*
Dit onderzoek richt zich op het verkrijgen van online gegevens (specifiek van Facebook) en gegevens welke zich fysiek bevinden op apparatuur (specifiek Apple telefoons en computers). De huidige wet- en/of regelgeving in het kader van digitale gegevens is geanalyseerd en vergeleken met een reële casus. Er is gekozen om de zaak van Dascha Graafsma te gebruiken als reële casus. Verder zijn er interviews afgenomen met: het onderzoeksteam van deze zaak, Digitale Nazorg, De Koninklijke Notariële Beroepsorganisatie en een voormalige digitaal rechercheur van de politie en nu particulier digitaal rechercheur.

Uit het onderzoek blijkt dat een opsporingsambtenaar bij verdenking van een ernstig misdrijf bevoegd is om digitale gegevensdragers in beslag te nemen en zonder tussenkomst van de Officier van Justitie (OvJ) onderzoek te doen aan dat voorwerp zolang er niet een min of compleet beeld wordt verkregen van bepaalde aspecten van het privéleven van de gebruiker. Voor smartphones geldt dat een opsporingsambtenaar, zonder toestemming van de OvJ, alleen een gering aantal gegevens mag raadplegen. Het inloggen in of het raadplegen van de app van Facebook is een vorm van binnendringen in een geautomatiseerd werk en kan inbreuk vormen op de soevereiniteit van een ander land. Als Facebookgegevens in het belang van de opsporing verkregen moeten worden kan er een internationaal rechtshulpverzoek gedaan worden.

Als uit het politieonderzoek blijkt dat er geen aanwijzingen zijn van een strafbaar feit dan hoeft er niet gehandeld te worden volgens de strafvordering. Door de afwezigheid van een strafvorderlijk belang is een opsporingsambtenaar niet bevoegd om Facebookgegevens te raadplegen of om deze te vorderen.

Het is onduidelijk of opsporingsambtenaren, op verzoek van de nabestaanden, onderzoek mogen verrichten aan digitale gegevensdragers als er geen aanwijzingen zijn van een strafbaar feit. Er moet daarom een procedure geïntroduceerd worden die nabestaanden de mogelijkheid biedt om een verzoek in te dienen bij de politie om onderzoek te laten verrichten aan de digitale gegevensdrager van een overledene bij overlijdensgevallen met suïcide als vermoedelijke toedracht.

Een rechtmatige erfgenaam is gerechtigd om zichzelf toegang te verschaffen tot een computer en telefoon van de overledene. Een rechtmatige erfgenaam heeft geen recht om zichzelf toegang te verschaffen tot het Facebookaccount van de overledene omdat de contractuele bepaling (algemene voorwaarden) tussen Facebook en de overleden persoon dit belemmert. De wetgevende macht moet het vermogensrecht en erfrecht zodanig uit te breiden dat er een wettelijke grondslag bestaat op basis waarvan erflaters kunnen bepalen wat er met hun data moeten gebeuren na overlijden.

Dit onderzoek geeft een beeld van de rechten van opsporingsambtenaren en nabestaanden in het kader van Apple apparatuur en Facebook. Maar mensen maken ook gebruik van andere elektronicabedrijven en online diensten. Er moet aanvullend onderzoek gedaan worden naar andere elektronicabedrijven en online diensten zoals Microsoft, WhatsApp, Gmail en clouddiensten zoals Dropbox.

Afkortingenlijst

Art.	Artikel
AVG	Algemene verordening gegevensbescherming
BW	Burgerlijk Wetboek
EVRM	Europees Verdrag voor de Rechten van de Mens
FA	Forensisch arts
FBI	Federal Bureau of Investigation
KNB	Koninklijke Notariële Beroepsorganisatie
MTI	More Than Investigation
NODOK	Nader onderzoek naar doodsoorzaak bij kinderen
OvJ	Officier van Justitie
RC	Rechter Commissaris
RUFADAA	Revised Uniform Fiduciary Access to Digital Assets Act
Sr.	Wetboek van strafrecht
Sv.	Wetboek van strafvordering
UFED	Universal Forensic Extraction Device
Wpg	Wet politiegegevens
Wjsg	Wet justitiële strafvorderlijke gegevens
z.d	zonder datum

Hoofdstuk 1: Inleiding

1.1 Aanleiding van het onderzoek

Casus voorbeeld

De 16-jarige Dascha Graafsma ging in de nacht van 28 november 2015 met haar vriendinnen naar het 16+ feestje 'Wintervibes' in Hilversum.[1] Rond 02:00 uur zegt Dascha tegen haar vriendinnen "dat ze even gaat plassen". Dascha kwam niet meer terug. Om 05:20 uur kwam Dascha in aanraking met een trein.[2] De forensische en tactische opsporing en de forensisch arts hebben geconcludeerd dat er sprake was van suïcide en de Officier van Justitie (OvJ) gaf het lichaam vrij. De familie gelooft de conclusie van de politie niet.[3]

Het komt steeds vaker voor dat nabestaanden twijfelen over de doodsoorzaak bij zaken waarbij de politie heeft geconcludeerd dat er waarschijnlijk sprake is van suïcide of een ongeluk. Vroeger had men babyboeken, fotoalbums en dagboeken. Tegenwoordig staat deze informatie op telefoons, laptops en social media.[4] Iedereen laat tegenwoordig een digitale erfenis achter op het moment dat ze overlijden.[5] Deze digitale erfenis bevat zeer privacygevoelige informatie die veel kan vertellen over een persoon. Die digitale informatie wordt ook steeds belangrijker voor de opsporing omdat het kan bijdragen aan de waarheidsvinding.[6] Nabestaanden vragen steeds vaker aan de politie om nader onderzoek te verrichten.[2] Maar als er geen aanwijzingen zijn van een strafbaar feit, mag de politie dan bijvoorbeeld zomaar een telefoon kraken en uitlezen? En waar ligt de grens?

Nabestaanden blijven vaak met veel vragen achter en hopen antwoord te krijgen op hun vragen door de digitale gegevens van de overledene in te zien. Nabestaanden kunnen terecht bij i-Finish om de inhoud van fysieke apparatuur inzichtelijk te maken. Maar i-Finish krijgt steeds meer verzoeken om ook de inhoud van social media en online accounts inzichtelijk te maken en veilig te stellen.

1.2 Probleemstelling

Uit de inleiding wordt duidelijk dat er in het kader van digitale erfenis twee belanghebbende partijen zijn, namelijk de nabestaanden en de opsporing. Nabestaanden willen beschikken over foto's en documenten van hun dierbare, noodzakelijk voor de afwikkeling of verwerking.[6] De opsporing wil beschikken over digitale data ten behoeve van de waarheidsvinding.[5] De opsporing mag bepaalde onderzoekshandelingen alleen inzetten wanneer er een redelijk vermoeden bestaat van een ernstig misdrijf.[7] Nabestaanden kunnen geen toegang krijgen tot de digitale gegevens omdat deze beveiligd zijn door toestelcodes, gebruikersnamen en wachtwoorden. De politie kan in sommige gevallen gebruik maken van bepaalde tools om smartphones en laptops te kraken.[8] Omdat het onduidelijk is in hoeverre opsporingsambtenaren gebruik mogen maken van digitale data als er (nog) geen aanwijzingen zijn van een misdrijf, hebben nabestaanden het gevoel dat er niet genoeg onderzoek wordt verricht.

Digitale Nazorg is een kenniscentrum met expertise op het gebied van technische oplossingen bij de digitale nalatenschap, zoals het inzichtelijk maken van gegevens op een laptop of mobiel.[9] Digitale Nazorg krijgt met de dienstverlening i-Finish steeds vaker verzoeken om gegevens van social media accounts inzichtelijk te maken. Het is voor i-Finish

onbekend wat er met deze data en accounts gebeuren na overlijden en wat commerciële bedrijf mogen doen met de data.

Bovendien wordt digitale data steeds beter beveiligd en wordt het moeilijker om de beveiliging te kraken. Voor commerciële bedrijven met diensten als i-Finish is het bijna onmogelijk om de nieuwste smartphones en laptops te kraken. Het is van belang om te achterhalen in hoeverre bedrijven als Apple moeten en kunnen helpen bij het verschaffen van toegang tot deze apparatuur. Het laatste jaar heeft i-Finish tientallen verzoeken gekregen tot aanvullende informatie voor nabestaanden naar aanleiding van zaken die door de politie zijn bestempeld als suïcide. Daarom wordt de focus van het onderzoek gelegd bij overlijdensgevallen met suïcide als vermoedelijke toedracht.

1.3 Doel

Het doel van dit onderzoek is om te achterhalen op welke wijze opsporingsambtenaren en nabestaanden zichzelf toegang kunnen verschaffen tot digitale data bij overlijdensgevallen met zelfdoding als vermoedelijke toedracht.

1.4 Hoofdvraag

De hoofdvraag van dit onderzoek luidt als volgt: op welke wijze kunnen opsporingsambtenaren en nabestaanden zichzelf op een juridisch correcte wijze toegang verschaffen tot digitale data bij overlijdensgevallen met suïcide als vermoedelijke toedracht?

1.5 Deelvragen

De hoofdvraag wordt beantwoord door middel van deelvragen:

- In hoeverre moet er sprake zijn van een strafbaar feit om onderzoek te mogen doen rondom de digitale data van een overledene?
- Wat is het verschil tussen onderzoek aan een fysieke, digitale gegevensdrager en onderzoek op een online social media account?
- Welke wetten rondom de privacy blijven gelden na overlijden?
- Welke rechten hebben nabestaanden rondom het social media account en digitale gegevensdragers van de overledene?
- In hoeverre belemmert de huidige wet- en/of regelgeving nabestaanden om toegang te krijgen tot de digitale nalatenschap?

1.6 Afbakening van het onderzoek

Om het onderzoek volledig uit te kunnen voeren binnen de gestelde termijn, is het van belang om aan te geven wat wel en wat niet tot het onderzoek behoort. Het onderzoek richt zich op digitale gegevensdragers en social media accounts. In het kader van social media wordt er alleen gekeken naar Facebook. Dit omdat vaak verzocht wordt aan i-Finish om Facebook accounts inzichtelijk te maken voor nabestaanden en het van belang is om te weten of dit mag. Bovendien blijkt uit de resultaten van het Nationaal Social Media Onderzoek van 2016,2017 en 2018 dat Facebook de laatste jaar een van de meest gebruikte social media platform is.[10,11,12] Uit een onderzoek van Oxford blijkt er in 2070 meer dode

dan levende mensen zullen zijn op Facebook.[13] Dit onderzoek richt zich op persoonlijke Facebook accounts. Zakelijke Facebook accounts en (zakelijke) Facebookpagina's worden buiten beschouwing gelaten.

Dit onderzoek houdt zich bezig met de juridische mogelijkheden voor het verkrijgen van digitale gegevens. Hierbij spelen de technische mogelijkheden een grote rol. De focus wordt gelegd op de juridische mogelijkheden, maar ook de technische mogelijkheden worden in acht genomen. Mensen kunnen verschillende apparaten gebruiken om toegang te krijgen tot Facebook, zoals computers. Omdat mensen niet elke keer opnieuw hun inloggegevens willen intoetsen, kiezen ze er vaak voor om deze op te slaan op de webbrowsers van hun computer of hun telefoon.[14] Het gevolg hiervan is dat, wanneer iemand toegang heeft tot een computer of telefoon, diegene ook vrij gemakkelijk toegang heeft tot je Facebook account. Daarom wordt er in dit onderzoek ook gekeken naar het elektronicabedrijf Apple. Er zijn verschillende soorten digitale gegevensdragers die toegang kunnen geven tot Facebook zoals tablets en smart-horloges, maar dit onderzoek beperkt zich tot computers en telefoons van Apple. Er is gekozen voor Apple omdat Apple apparatuur zo goed beveiligd is, dat het steeds moeilijker wordt om Apple apparatuur te kraken.[15] De opsporing kan in sommige gevallen gebruikmaken van technische tools als Axiom Gray key om toegang te krijgen tot Apple apparatuur. Deze tool is alleen beschikbaar voor de politie.[16] Voor commerciële bedrijven met diensten als
i-Finish is het momenteel bijvoorbeeld niet mogelijk om de Apple software iOS 8 of hoger te kraken.

Hoofdstuk 2: Theoretisch kader

2.1 Privacy na overlijden

Het recht houdt zich al jaren bezig met het beschermen van de privacy. Het recht op privacy is opgenomen in artikel 10 van de Nederlandse Grondwet: "Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer".[17] Vervolgens kwam in 1989 de Wet persoonsregistraties tot stand. Deze wet stelt regels met betrekking tot het verwerken van persoonsgegevens.[17] In 1995 werd de beschermingsrichtlijn van het Europees Parlement en de Raad opgesteld. Europese richtlijnen treden niet direct in, maar moeten door de lidstaten worden omgezet in nationale wetgeving. In 2001 heeft Nederland deze richtlijn omgezet in de Wet bescherming persoonsgegevens.[18] In 2016 werd door het Europees Parlement en de Raad de Algemene Verordening Gegevensbescherming (AVG) vastgesteld. De AVG heeft wel een directe werking omdat het een verordening is.[19] In overweging 27 van de AVG staat vermeld dat de verordening niet van toepassing is op persoonsgegevens van overleden individuen, maar dat lidstaten zelf regels mogen opstellen voor het verwerken van deze gegevens.[20] Nederland, Oostenrijk, België, Tsjechië, Duitsland, Finland, Ierland, Polen, Zweden en het Verenigd Koninkrijk hebben (nog) geen regels opgesteld met betrekking tot persoonsgegevens van overledenen. Denemarken, Frankrijk, Italië, Spanje, Hongarije en Slowakije hebben dit wel gedaan.[21] In bijlage 1 wordt een tabel weergegeven van de regelgeving die de landen hebben opgesteld voor het verwerken van gegevens van overledenen.

Er zijn wel andere wetten die wel na de dood gelden. Art. 272 Sr. stelt dat indien iemand die vanuit zijn ambt zijn beroepsgeheim opzettelijk schendt, wordt gestraft.[22] Op basis van art. 7:457 BW moet het beroepsgeheim ook na overlijden in acht genomen worden.[23] Of nabestaanden wel of geen inzage mogen krijgen, was niet altijd even duidelijk. De Hoge Raad heeft in 2008 besloten dat inzage in het medisch dossier, en daarmee schending van het beroepsgeheim (art. 272 Sr.) van een overledene, toegestaan is wanneer een patiënt tijdens leven toestemming hiervoor heeft gegeven of als er sprake is van een veronderstelde toestemming.[24] Verder zijn er regels voor wat er met een lijk mag gebeuren. Dit staat opgesteld in de Wet op de lijkbezorging.[25] Ook blijft het auteursrecht op grond van artikel 37 van de auteurswet tot zeventig jaar na het overlijden van de maker.[26] In de auteurswet wordt ook het portretrecht geregeld. Het portretrecht is van toepassing op afbeeldingen waarop een persoon herkenbaar is afgebeeld. Het gaat dus niet alleen om een gezicht van een persoon, maar ook om kenmerken waaruit je een persoon kunt herkennen. Het portretrecht geldt tot tien jaar na overlijden.[27]

Op het internet geldt de auteurswet nog steeds. Maar op social media platforms gelden andere regels. Dit komt omdat je bij het aanmaken van een account akkoord moet gaan met de servicevoorwaarden van het platform.[28] Bij Facebook is het zo dat je het platform een licentie geeft om jouw werk te gebruiken. Zo staat er in de servicevoorwaarden van Facebook vermeld dat een gebruiker *"een niet-exclusieve, overdraagbare, sublicentieerbare, royaltyvrije en wereldwijde licentie voor het hosten, gebruiker, distribueren, wijzigen, uitvoeren, kopiëren, openbaar uitvoeren of weergeven, vertalen en maken van afgeleide werken van de gebruiker."*[29]

Dit is ook nodig, anders zou Facebook het werk niet mogen tonen op hun website. Dit betekent niet dat iemand een afbeelding van een ander mag downloaden en vervolgens zelf mag gebruiken. Om dat te kunnen doen is op grond van het auteursrecht, toestemming nodig.[30]

2.2 Digitale nalatenschap

Het geheel van bezittingen en schulden die een persoon achterlaat op het moment dat iemand komt te overlijden, wordt nalatenschap genoemd.[31] Met de opkomst van technologie wordt er gesproken over een "*gedigitaliseerde samenleving*".[32] Het gevolg hiervan is dat wij steeds minder fysieke nalatenschap achterlaten en meer digitale nalatenschap. Gezien de toenemende statistieken met betrekking tot online gedrag wordt het belang om digitale data na het overlijden te beschermen, steeds groter. Onderzoeker Natascha Cu erkent dit probleem en heeft gekeken naar welke methodes er bestaan om de privacy van een overledene te beschermen.[33] Zo kan er gebruik gemaakt worden van de contractwetgeving-methode. Het probleem van deze methode is dat de social media gebruiker tijdens leven akkoord is gegaan met de servicevoorwaarden van de aanbieder, die vaak in het voordeel van de aanbieder zijn opgesteld.[34] Een andere mogelijke methode is de digitale activa van een persoon te behandelen als eigendom. Het moet echter niet zo zijn dat de digitale activa onbedoeld wordt overgedragen aan de nabestaanden, aangezien digitale activa persoonlijke informatie kunnen bevatten terwijl dat bij andere eigendommen niet het geval is. Volgens Natascha Cu moet de bestaande wetgeving uitgebreid worden, zodat de privacy van overledenen beschermd wordt.[33]

Als er wordt gekeken naar het Nederlandse erfrecht, dan loopt Nederland ten opzichte van Amerika achter. Er is geen wet die duidelijk aangeeft wat digitale activa zijn en wat hieronder valt, zoals de Amerikaanse wetgeving dat doet.[34] Het gevolg hiervan is dat digitale activa, nu in Nederland, op dezelfde manier moeten worden geërfd als andere activa. De Amerikaanse wetgeving wordt later besproken. Er wordt eerst gekeken naar het Nederlands erfrecht.

Er wordt in Nederland onderscheid gemaakt tussen twee soorten erfrecht, namelijk het testamentaire erfrecht en het versterferfrecht.[35] Als de overledene voor zijn overlijden een testament heeft opgemaakt, dan geldt het testamentaire erfrecht. Een testament is een juridisch document waarbij een persoon aangeeft wie wat erft. Ook kan in een testament aangegeven worden wie het erfrecht afhandelt. In het geval dat de overledene geen testament heeft opgemaakt, gelden de standaardregels van het versterfrecht.[35] Hierbij bepaalt de wet wie wat erft. Dit staat in het Burgerlijk Wetboek 4. Volgens art. 4:10 BW. zijn er vier groepen van erfgenamen:[36]

1. De echtgenoot/geregistreerd partner samen met de kinderen
2. De ouders samen met de broers en zusters
3. De grootouders
4. De overgrootouders

In het geval dat de eerste groep niet van toepassing is, heeft de volgende groep recht op de nalatenschap, et cetera.[36] Hierbij worden alle bezittingen, maar ook alle schulden overgedragen aan de erfgenaam.

De erfgenaam is daarbij verantwoordelijk voor het afhandelen van de erfenis.[35] Erfgenamen kunnen ook iemand anders met een volmacht machtigen om de erfenis namens hen af te handelen. Deze persoon wordt ook wel de executeur genoemd. Er zijn vijf soorten volmachten, namelijk de algehele, bijzondere, notariële, onderhandse en bankvolmacht.[37] Om de erfenis af te handelen moet een erfgenaam altijd bewijzen dat hij of zij inderdaad de rechtmatige erfgenaam is. Dit kan gedaan worden door een verklaring van erfrecht te tonen. Een verklaring van erfrecht wordt opgesteld door een notaris.[38]

Zoals in het begin van de paragraaf al werd benoemd, heeft de Amerikaanse wetgeving regels opgesteld voor het omgaan met de digitale nalatenschap.[34]
In 2015 heeft de 'Uniform Law Commission' van Amerika de wet 'Revised Uniform Fiduciary Access to Digital Assets Act' (RUFADAA) herzien en aangenomen. Eenenveertig staten van Amerika en de U.S. Virgin Islands hebben de wet overgenomen. De RUFADAA definieert 'digitale activa' als "*elektronische gegevens waarbij een individu een recht of een belang heeft*".[34] Dit kunnen gegevens zijn die opgeslagen staan op een computer of een ander digitaal apparatuur of de gegevens die op een website zijn geplaatst.

De RUFADAA bepaalt dat de servicevoorwaarden van de online dienst van toepassing zijn, mits de gebruiker 'wettelijke toestemming' heeft gegeven omtrent het openbaar maken van zijn of haar digitale activa. De RUFADAA stelt regels voor het opstellen van een verzoek tot openbaarmaking.[34] De regels verschillen per situatie, maar in het algemeen zijn de volgende documenten van toepassing:

1. Een verzoek in schriftelijke of elektronische vorm aan de online dienst
2. Een akte van overlijden of andere vorm van bewijs van het overlijden
3. Een gecertificeerd document waaruit blijkt dat de persoon de rechtmatige erfgenaam is van (een deel van de) de digitale nalatenschap.

In het geval dat de originele gebruiker tijdens leven toestemming heeft gegeven tot openbaring, heeft een erfgenaam toegang tot "de inhoud van elektronische communicatie". Wanneer de originele gebruiker geen wettelijke toestemming heeft gegeven, kan een persoonlijke vertegenwoordiger namens de RUFADAA de online dienst verzoeken om een "register van elektronische communicatie dat door de gebruiker werd verzonden of ontvangen" openbaar te stellen.[34] Dit is niet hetzelfde als de "inhoud van elektronische communicatie". Een "register van elektronische communicatie" zegt iets over de communicatie, maar betreft niet de inhoud van de communicatie zelf. Een register van mailcommunicatie waarbij te zien is met wie en wanneer iemand gemaild heeft, is een vorm van een "register van elektronische communicatie". Er is pas sprake van "inhoud van elektronische communicatie" op het moment dat er inzicht wordt verkregen in de inhoud van de mail zelf.[34]

Zoals eerder vermeld, kan iemand pas gebruik maken van een online dienst wanneer zij akkoord gaan met de servicevoorwaarden van die dienst. De meeste mensen lezen de servicevoorwaarden niet omdat ze het teveel tekst vinden.[39] Servicevoorwaarden bevatten regels over wat er met de data van het account wordt gedaan en wie er toegang mag krijgen tot het account.[28]
In de servicevoorwaarden van Facebook staat vastgesteld dat het niet toegestaan is om:[24]

- inloggegevens van het account te delen met anderen
- anderen toegang te geven tot het account
- het account over te dragen aan anderen

zonder toestemming van Facebook.

Facebook heeft drie opties voor accounts van overleden gebruikers.[29]

1. Facebook account open laten
2. Facebook account een herdenkingsstatus geven
3. Facebook account verwijderen

Een naaste familielid kan een verzoek indienen bij Facebook om het Facebook account van de overledene te verwijderen of een herdenkingsstatus te geven. Een gebruiker kan van tevoren ook zelf aangeven welke van de bovengenoemde drie opties zijn of haar voorkeur heeft.[40]

2.3 Toegang verschaffen tot digitale gegevens

Apple is een elektronicabedrijf dat computers, telefoons, muziekspelers, tablets en softwares ontwikkelt. Apple zorgt ervoor dat elke versie van hun apparatuur beter is beveiligd dan de vorige.[15] Het bedrijf beweert dat zij zelf de beveiliging van hun telefoons niet kunnen kraken en dat zij geen wachtwoorden opslaan.[41] Dit staat soms de opsporing in de weg, zoals blijkt uit een zaak in San Bernardino.[42] Op 2 december 2015 vond er een aanslag plaats in San Bernardino. Er werd een iPhone 5c aangetroffen op het lichaam van een vermoorde terrorist. De Federal Bureau of Investigation (FBI) kon de iPhone niet ontgrendelen dankzij het sterke versleutelingssysteem van Apple. Dit was niet de eerste keer dat het voor de FBI technisch onmogelijk was om een telefoon van Apple te kraken. De FBI verzocht Apple - zowel via de pers als via de rechtbank - om software te ontwikkelen die gebruikt kan worden door de FBI om de iPhone 5c te ontgrendelen. Gezien het feit dat de software dan ook gebruikt kan worden om andere telefoons van Apple te kraken, wilde Apple niet meewerken.[42]

Art. 138ab Sr. stelt dat iemand schuldig is aan computervredebreuk op het moment dat iemand binnendringt in een geautomatiseerd werk.[43] Volgens art. 80sexies Sr. wordt onder geautomatiseerd werk verstaan “een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen.”[22] In de memorie van toelichting van de Wet Computercriminaliteit III werden voorbeelden van geautomatiseerd werk benoemd, namelijk computers, tablets en smartphones.[44] Er wordt een hogere straf gesteld voor degenen die na het binnendringen ook gegevens die staan opgeslagen in het systeem, verwerken.[22] De wet geeft geen duidelijke definitie voor de term ‘binnendringen’. Dit betekent dat de rechter zelf kan beslissen of een bepaalde handeling valt onder de term ‘binnendringen’. Art. 138ab Sr. geeft wel een paar voorbeelden van binnendringen:

A. door het doorbreken van een beveiliging,

B. door een technische ingreep,
C. met behulp van valse signalen of een valse sleutel, of
D. door het aannemen van een valse hoedanigheid.

In 2018 werd een man veroordeeld voor het hacken van online accounts van bekende Nederlanders.[45] De rechtbank achtte bewezen verklaard dat de man: “opzettelijk en wederrechtelijk in een gedeelte van een geautomatiseerd werk, te weten twee Facebook accounts en een Gmail account binnen heeft gedrongen.” Dit werd bereikt door middel van valse signalen of een valse sleutel (zoals neergelegd in art. 138ab Sr.), te weten een onrechtmatig verkregen wachtwoord.

2.4 Digitaal onderzoek in de opsporing

Digitaal forensisch onderzoek is een vorm van forensisch onderzoek waarbij gebruik gemaakt wordt van digitale sporen.[46] Bij elk vorm van forensisch onderzoek is het belangrijk om breed te denken om tunnelvisie te voorkomen. Hypotheses en scenario’s kunnen daarbij een belangrijk tool zijn.[47] Hypotheses zeggen iets over “wat” er is gebeurd. De bijbehorende scenario’s geven aan “hoe” iets is gebeurd. Scenario’s beschrijven de handelingen die mogelijk plaats hebben gevonden voor, tijdens en na een misdrijf. Bij een lijkvinding worden de vier basis-hypotheses opgesteld: moord, ongeval, natuurlijke dood, suïcide.[48] Aan de hand van de aangetroffen sporen worden de hypotheses/scenario’s getoetst. Er wordt gesproken van falsificeren wanneer het aangetroffen bewijsmateriaal een bepaalde hypothese/scenario niet ondersteunt. Wanneer bewijsmateriaal een hypothese/scenario ondersteunt, wordt dit verificatie genoemd. Het is belangrijk dat er niet alleen gefocust wordt op het verifiëren van een bepaalde hypothese/scenario.[48]

Politieambtenaren hebben bevoegdheden die nabestaanden niet hebben.[7] Daarmee kan een politieambtenaar opsporingshandelingen uitvoeren die inbreuk maken op de (grond)rechten van een burger. Een opsporingsambtenaar moet altijd vooraf zijn handelingen toetsen op proportionaliteit en subsidiariteit.[7] Daarbij moet besloten worden of er een redelijke verhouding bestaat tussen het beoogde doel en de inbreuk op de rechten van die persoon (proportionaliteitsbeginsel) en of de gekozen methode het minst ingrijpend is (subsidiariteitsbeginsel).[7] Artikel 8 van het Europees Verdrag voor de rechten van de Mens (EVRM) zorgt ervoor dat mensen het recht hebben op respect voor familie- en gezinsleven.[49] Lid 2 van dit artikel eist dat er geen inbreuk gemaakt mag worden op dit recht, mits dit noodzakelijk is in het belang van:

- De nationale of openbare veiligheid
- Het economisch welzijn van het land
- Het voorkomen van wanordelijkheden en strafbare feiten
- De bescherming van de gezondheid of de goede zeden of de de rechten en vrijheden van anderen

Krachtens art. 96 Sv. is een opsporingsambtenaar bevoegd om op heterdaad van een strafbaar feit of in geval van verdenking van een misdrijf als omschreven in art. 67 lid 1 Sv. de daarvoor vatbare voorwerpen in beslag te nemen en daartoe elke plaats (met uitzondering van een woning) te betreden.[43] Art. 94 Sv. bepaalt dat voorwerpen vatbaar zijn voor inbeslagneming wanneer deze:

- de waarheid aan het licht kunnen brengen

- het wederrechtelijk verkregen voordeel aan kunnen tonen
- voor verbeurdverklaring of onttrekking aan het verkeer kunnen worden bevolen.

Op grond van art. 94 Sv. kan er onderzoek verricht worden aan in beslag genomen voorwerpen.[43] In 1994 heeft de Hoge Raad bepaald dat gegevens in een computer daarvan niet zijn uitgezonderd.[50] Dat er zich ook mogelijke privacygevoelige gegevens bevinden op een laptop, is samengaand met de inbeslagneming.[51]

In 2017 is beoordeeld dat hetzelfde geldt voor smartphones.[52] De advocaat vond dit een schending van artikel 8 EVRM. Volgens de Hoge Raad maakt onderzoek aan een smartphone een beperkte inbreuk op de privacy. Wanneer een onderzoeksmethode beperkte inbreuk maakt op de privacy van een persoon, kan een opsporingsambtenaar zonder tussenkomst van de OvJ zelf beoordelen of het onderzoek nodig is. Op het moment dat een onderzoek meer dan een beperkte inbreuk maakt op de privacy, is vooraf toestemming nodig van de OvJ.

De Hoge Raad heeft bepaald dat er sprake is van een meer dan beperkte inbreuk op het moment dat “een min of meer compleet beeld is verkregen van bepaalde aspecten van het persoonlijk leven van de gebruiker van de gegevensdragers of het geautomatiseerd werk.” In 2018 moest de Hoge Raad bepalen of er sprake was van een meer dan beperkte inbreuk op de privacy op het moment dat een smartphone wordt uitgelezen met een software als XRY.[53] De raadsman beargumenteerde dat een smartphone meer persoonlijke gegevens bevat dan een klassieke mobiele telefoon. De Hoge Raad merkte op dat door gebruik te maken van XRY alle gegevens van de telefoon inzichtelijk worden gemaakt. Daarom is er geen sprake meer van het raadplegen van een gering aantal gegevens en wordt er een meer dan beperkte inbreuk gemaakt op de persoonlijke levenssfeer. Het Hof oordeelde dat daarvoor vooraf toestemming nodig is van de OvJ.[53] Als dit niet wordt gedaan, dan is dit een schending van artikel 8 EVRM.

Sinds 1 maart 2019 is de Wet computercriminaliteit III van toepassing.[44] Deze wet zorgt voor nieuwe bevoegdheden voor daartoe aangewezen opsporingsambtenaren om heimelijk en op afstand binnen te dringen in geautomatiseerd werk. Hiernaast maakt de wet het mogelijk om vervolgens diverse onderzoekshandelingen toe te passen. Zo kan er binnengedrongen worden in de laptop van een verdachte en kan de verdachte gelokaliseerd en/of afgeluisterd worden.[44] Het binnendringen in een geautomatiseerd werk maakt een grote inbreuk op de privacy van de verdachte. Daarom mag dit alleen gedaan worden met toestemming van de OvJ.[7]

Voordat de bevoegdheid ingezet wordt, moet deze eerst getoetst worden aan de proportionaliteit en subsidiariteit. Daarbij worden de doelen, de beschikbare technieken en middelen, de alternatieve middelen en de mate van inbreuk op de privacy in kaart gebracht.[7] Om dit in kaart te brengen mag er gebruik gemaakt worden van verkeersgegevens en de bevoegdheid tot het aftappen van communicatie. Vervolgens wordt het voorstel aan de Centrale Toetsingscommissie voorgelegd en moet de OvJ een machtiging vorderen bij de rechter-commissaris.[7,44]

De bevoegdheid om binnen te dringen in een geautomatiseerd werk is alleen van toepassing bij verdenking van misdrijven zoals vermeld in art. 67 lid 1 sv [44] Voor het verwerken van gegevens na het binnendringen wordt vereist dat er sprake moet zijn van verdenking van een misdrijf waarop minimaal acht jaar gevangenisstraf wordt gesteld of een misdrijf dat kan zorgen voor ernstige inbreuk op de rechtsorde.[44]

De bevoegdheid om vanaf afstand binnen te dringen in een geautomatiseerd werkt brengt met zich mee dat er toegang verkregen kan worden tot een werk dat staat in het buitenland. Op het moment dat het bekend is dat bepaalde gegevens in het buitenland staan, moet er een rechtshulpverzoek gedaan worden.[54]

Het is niet altijd mogelijk om te achterhalen waar specifieke data staan opgeslagen. De "aanwijzingen voor de internationale aspecten van de bevoegdheid ex art. 126nba Sv." is op 26 februari 2019 gepubliceerd.[54] Hieruit blijkt dat wanneer de locatie onbekend is, er onderzocht moet worden of de tijd en moeite van vaststellen van de locatie in verhouding staat tot de noodzaak van optreden. Als dat niet het geval is, dan moet de opsporingsambtenaar handelen alsof de gegevens zijn opgeslagen in Nederland. Wanneer een verzoek tot rechtshulp is gedaan maar de reactie niet afgewacht kan worden, is het mogelijk om zonder toestemming te handelen. Dit moet afgewogen worden door de OvJ en moet vermeld worden aan de rechter-commissaris.[54]

Een OvJ is krachtens art. 126n Sv bevoegd om een communicatiedienst te vorderen om gegevens van een gebruiker en het communicatieverkeer van die gebruiker te verstrekken, als er sprake is van een verdenking van een misdrijf en de gegevens van belang zijn voor het onderzoek.[43] Maar dit is alleen van toepassing op Nederlands grondgebied.[44] Als een aanbieder niet in Nederland is gevestigd, kan er een verzoek gedaan worden via het Europees onderzoeksbevel (EOB) aan alle landen van de Europese Unie met uitzondering van Denemerken en Ierland.[7] De EOB is bedoeld om verzoeken te vereenvoudigen en te versnellen.[55] Als de EOB niet van toepassing is, moet er een rechtshulpverzoek ingediend worden.[7]

Facebook is gevestigd in Ierland. Het Europees onderzoeksbevel is niet van toepassing op Ierland. Facebook heeft wel een 'Law Enforcement Online Request System'.[56] De politie kan gebruikmaken van dit systeem om verzoeken in te dienen voor het inzien van Facebookgegevens. Facebook verstrekt alleen accountgegevens in overeenstemming met de toepasselijke wetgeving en hun servicevoorwaarden.[56] Er kan een verzoek tot bewaring accountgegevens gedaan worden. De gegevens worden dan voor 90 dagen bewaard. Facebook geeft expliciet aan wat voor type gegevens ze kunnen verschaffen aan de politie.[57] Facebook kan de volgende informatie verstrekken aan de politie:

- Basisgegevens van de gebruiker (e-mailadres, telefoonnummer en een logboek van de dagen en tijden dat iemand heeft ingelogd). Het logboek betreft meestal gegevens van twee à drie dagen voordat het verzoek is verwerkt.
- Uitgebreide informatie van de gebruiker. Dit betreft informatie zoals: Wall posts, vriendenlijst, evenementen en video's.
- Foto's van de gebruiker: Geüploade foto's waarbij de gebruiker is getagd en foto's die de gebruiker zelf heeft geüpload.

- Informatie over een groep: informatie over de maker, de beheerder en de indeling van de groep.
- Privéberichten: berichten van Facebook Messenger indien deze bewaard zijn.
- IP-logboek: deze gegevens zijn vaak onvolledig.

Apple heeft aparte richtlijnen voor het opvragen van informatie door overheidsinstanties die zich buiten de Verenigde Staten bevinden.[41] Er wordt duidelijk aangegeven dat Apple geen toegang heeft tot toegangscodes van Apple-apparaten.[41] Dit betekent dat Apple geen toestellen kan ontgrendelen. Bovendien kan Apple geen data extraheren uit een apparaat dat gebruik maakt van de software iOS 8 of hoger.[41] Gebruikers worden door Apple op de hoogte gebracht op het moment dat er een verzoek is ingediend dat betrekking heeft op de gegevens van de gebruiker. Dit wordt niet gedaan wanneer de wet dit verbiedt.[41]

Apple kan wel de volgende informatie verstrekken aan overheidsinstanties:
- Gegevens die door de gebruiker worden verstrekt op het moment dat de gebruiker een Apple-apparaat registreert.
- iTunes (mediaspeler en mediabibliotheek van Apple): abonnee informatie, informatie over de gemaakte aankopen en downloads en logboek van de gemaakte verbindingen met IP-adressen
- Find my iPhone (applicatie van Apple die de locatie van jouw Apple apparatuur bijhoudt): logboek van de gemaakte verbindingen met de app. Informatie over locaties van het apparaat kan Apple niet achterhalen.
- Mac address: een uniek identificatienummer voor netwerkinterfaces (Bluetooth,Wi-Fi)
- Apple Online Store: alle aankopen en downloads van de Apple Online Store
- E-mail: een logboek van het mailverkeer van iCloud.
- iCloud (cloud-opslagdienst van Apple): een logboek van de gemaakte verbindingen met iCloud.

Voor de volgende informatie is een gerechtelijk bevel nodig:
- Facetime (Videobel-applicatie van Apple): informatie van Facetime is versleuteld door end-to-end encryptie. Apple kan deze niet ontsleutelen. Apple kan wel een logboek verstrekken met data die aantonen wanneer een FaceTime-Oproep plaats heeft gevonden.
- iMessage(chat-applicatie van Apple): informatie van iMessage is versleuteld door end-to-end encryptie. Apple kan deze niet ontsleutelen. Apple kan een logboek verstrekken met de ‘query verzoeken’. Op het moment dat een gebruiker een bericht stuurt, wordt er een query verzonden naar de Apple-server om te bepalen of deze geschikt is voor iMessage. Apple kan echter niet op basis van dit logboek achterhalen of er daadwerkelijk communicatie heeft plaatsgevonden via iMessage. De logboeken worden standaard voor 30 dagen bewaard. Om ervoor te zorgen dat data niet verloren gaan, kan er een verzoek tot bewaring ingediend worden. Nadat dit verzoek is ontvangen, worden de aangevraagde gegevens voor 90 dagen bewaard.

2.5 Het inzien van politiegegevens

In de Wet politiegegevens (Wpg) wordt beschreven hoe opsporingsambtenaren moeten omgaan met persoonsgegevens.[58] Artikel 1 van de Wpg beschrijft de definitie van persoonsgegevens: *Elk persoonsgegeven (alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon) dat wordt verwerkt in het kader van de uitvoering van de politietaak.*[58]

Op het moment dat persoonsgegevens worden verwerkt in het kader van een strafvorderlijk onderzoek, worden deze strafvorderlijke gegevens genoemd.[59] De regels voor het verwerken van deze gegevens worden geregeld in de Wet Justitiële strafvorderlijke gegevens (Wjsg).[59] Omdat gegevens van een overleden personen geen persoonsgegevens zijn, kunnen gegevens van een overledene verkregen in een strafrechtelijk onderzoek geen strafvorderlijke gegevens zijn.
De Wjsg biedt alleen grondslag voor het verstrekken van gegevens van overledenen op het moment dat er ook sprake is van gegevens van andere natuurlijke personen. Wanneer dit niet het geval is, speelt de geheimhoudingsplicht van de OvJ een rol.[59] Artikel 13 van de Wet op de rechterlijke organisatie acht dat de geheimhoudingsplicht behouden moet worden *'voorzover enig wettelijke voorschrift hen tot mededeling verplicht of uit hun ambt de noodzaak tot mededeling voortvloeit'*.[60]

Bij overlijdensgevallen waarbij geconcludeerd is dat het meest waarschijnlijk een suïcide of ongeluk betreft, kan het voorkomen dat nabestaanden twijfelen aan de doodsoorzaak en kan het van belang zijn om gegevens in te zien ten behoeve van rouwverwerking.[59] Nabestaanden kunnen een gemotiveerd verzoek sturen naar de OvJ om inzage te krijgen in het onderzoeksdossier. Bij het behandelen van het verzoek moet de OvJ een belangenafweging doen tussen het belang van inzage en de privacybelangen van anderen.[59]

Hoofdstuk 3: Onderzoeksopzet

In dit hoofdstuk wordt de opzet van het onderzoek besproken. Als eerste worden de belangrijkste punten van het theoretisch kader besproken.

Uit het theoretisch kader blijkt dat een opsporingsambtenaar bij verdenking van een ernstig misdrijf bevoegd is om digitale gegevensdragers in beslag te nemen en zonder tussenkomst van de OvJ onderzoek te doen aan dat voorwerp zolang er niet een min of compleet beeld wordt verkregen van bepaalde aspecten van het privéleven van de gebruiker van dat geautomatiseerd werk.[52] Verder blijkt dat er recent nieuwe wetten zijn ingevoerd met betrekking tot het binnendringen in een geautomatiseerd systeem.[44] Verder is de internetinfrastructuur zo ingewikkeld geworden dat het vaak niet of moeilijk te bepalen is waar bepaalde data staan opgeslagen.[54] Ook komt in het theoretisch kader naar voren dat er in Nederland weinig is geregeld voor het erven van een digitaal activum en dat nabestaanden sterk afhankelijk zijn van de algemene voorwaarden van de online dienst.[31]

De hoofdvraag van het onderzoek luidt als volgt: *op welke wijze kunnen opsporingsambtenaren en nabestaanden zichzelf op een juridisch correcte wijze toegang verschaffen tot digitale data bij overlijdensgevallen met suïcide als vermoedelijke toedracht?*

Naast het bestuderen van de bestaande wet- en/of regelgeving en jurisprudentie wordt achterhaald hoe deze wet- en/of regelgeving in de praktijk wordt toegepast. Dit wordt bereikt door interviews af te nemen en door een reële zaak te bestuderen. Er is gekozen voor de zaak van Dascha Graafsma.

Toelichting zaak Dascha Graafsma
De vader van Dascha was het niet eens met de conclusie van de politie en heeft een eigen onderzoeksteam samengesteld. Het doel was te achterhalen wat er die nacht is gebeurd met Dascha.[3] Het onderzoeksteam is verdergegaan als More Than Investigation (MTI). In april 2019 heeft MTI een rapportage uitgebracht waarin de onderzoeksresultaten van de politie worden vergeleken met de bevindingen van MTI.[3] In dit rapport komt ook het digitale onderzoek aan bod. Er is gekozen voor deze zaak omdat het rapport van MTI een beeld geeft van hoe de politie in de praktijk gebruik maakt van digitale gegevens bij dit soort overlijdensgevallen.

Deelvraag 1: *In hoeverre moet er sprake zijn van een strafbaar feit om onderzoek te mogen doen rondom de digitale data van een overledene?*
Deelvraag 2: *Wat is het verschil tussen onderzoek aan een fysieke, digitale gegevensdrager en onderzoek op een online social media account?*
Deelvraag 3: *Welke wetten rondom de privacy blijven gelden na overlijden?*

Als eerst wordt de huidige wet- en/of regelgeving bestudeerd om te achterhalen onder welke voorwaarden opsporingsambtenaren digitale data mogen onderzoeken. Uit het theoretisch kader wordt duidelijk dat opsporingsambtenaren bevoegdheden hebben die ingezet kunnen worden als er sprake is van een verdenking van een strafbaar feit. Het is van belang om te achterhalen wanneer gesproken kan worden van een “verdenking van een strafbaar feit”.

Er wordt een schema gemaakt van de inzet van de politie bij overlijdensonderzoeken, wat voor invloed deze mensen hebben op het proces en hoe dit kan leiden tot een “verdenking van een strafbaar feit”.

Vervolgens wordt aan de hand van de rapportage van MTI en een interview met MTI bepaald in welk stadium van het onderzoek de politie heeft besloten om de digitale gegevens van Dascha te onderzoeken en of dit overeenkomt met de huidige wet- en/of regelgeving. Verder is het van belang om in acht te nemen dat Dascha in 2015 is overleden. Er moet daarom rekening gehouden worden met het feit dat digitale data tegenwoordig beter is beveiligd. Daarom moet er onderzocht worden wat opsporingsambtenaren mogen doen met bekende wachtwoorden en hoe bedrijven als Apple en Facebook samenwerken met de Nederlandse politie. Bovendien moet er bepaald worden of de recente wet computercriminaliteit III nieuwe mogelijkheden biedt.

Bij overlijdensgevallen met suïcide als vermoedelijke toedracht kan het voorkomen dat er, op het eerste oog, geen duidelijke aanwijzingen zijn van een misdrijf. Er moet worden bepaald wat de mogelijkheden zijn in het kader van digitaal onderzoek als er (nog) geen duidelijke aanwijzingen zijn van een misdrijf. Er wordt gekeken naar hoe de privacy van een overledene wordt beschermd en hoe dit een mogelijkheid kan bieden voor opsporingsambtenaren om toegang te krijgen tot de digitale data van een overledene. Naast MTI wordt er ook een interview gehouden met Remon Verkerk, een voormalige digitaal rechercheur van de politie en nu particulier digitaal rechercheur, om inzicht te krijgen in hoe digitaal rechercheurs van de politie te werk gaan en waar nabestaanden volgens hem tegenaan lopen.

Deelvraag 5: *Welke rechten hebben nabestaanden rondom het social media account en digitale gegevensdragers van de overledene?*
Deelvraag 6: *In hoeverre belemmerd de huidige wet- en/of regelgeving nabestaanden om toegang te krijgen tot de digitale nalatenschap?*

Voor de nabestaanden is het van belang om te achterhalen van wie digitale data zijn en hoe dit overgedragen kan worden. Zoals eerder besproken zijn digitale data vrijwel altijd beveiligd met wachtwoorden. Er moet bepaald worden wat nabestaanden mogen doen met bekende wachtwoorden en wat nabestaanden kunnen doen als het wachtwoord niet bekend is. Dit wordt bepaald aan de hand van de bestaande wet- en/of regelgeving, jurisprudentie, het rapport van MTI en aan de hand van de bovengenoemde interviews. Er wordt ook een interview gehouden met Digitale Nazorg om te achterhalen waar zij en hun klanten tegenaan lopen en hoe bedrijven als Apple hier hulp bij bieden. Verder wordt er een interview gehouden met de Koninklijke Notariële Beroepsorganisatie om te kijken hoe het erfrecht een rol speelt bij het inzien van digitale gegevens van overledenen. De interviews zijn semi-gestructureerd opgebouwd. Bij een semi-gestructureerd interview zijn de vragen algemener geformuleerd dan bij een gestructureerd interview. Dit zorgt ervoor dat er ruimte is om vervolgvragen te stellen, wat zorgt voor meer informatie.[62]
De uitwerking van de interviews kan op aanvraag ingezien worden.

Aan de hand van de antwoorden op de deelvragen wordt er in de conclusie antwoord gegeven op de hoofdvraag en worden eventueel aanbevelingen gedaan.

Hoofdstuk 4: Resultaten en discussie

In dit hoofdstuk worden de resultaten van het onderzoek besproken. De resultaten worden aan de hand van de zaak van Dascha Graafsma besproken. De zaak start bij een melding dat een persoon aangereden is door een trein.

4.1 Van melding tot het starten van een strafrechtelijk onderzoek

De politie wordt ingeschakeld bij alle gevallen van onverklaard of niet-natuurlijk overlijden, behalve als er sprake is van een verklaarde niet-natuurlijk dood in een zorginstelling of als er sprake is van euthanasie door een arts. Een niet-natuurlijk dood is een overlijden als gevolg van bijvoorbeeld een ongeval of geweld of een andere oorzaak van buitenaf.[62]
Dascha Graafsma is aangereden door een trein. Dit is een niet-natuurlijk overlijden en dus moet de forensische opsporing, de tactische recherche en de forensisch arts ter plekke komen. Deze drie worden ingezet omdat aanwijzingen voor een misdrijf forensisch, tactisch of medisch van aard kunnen zijn.[3]

Het onderzoek kan lijden tot vier typen conclusies.[62]

- *Natuurlijk overlijden*

Er wordt geen contact opgenomen met de OvJ.

- *Niet overtuigd van natuurlijke dood, maar geen aanwijzingen voor een misdrijf*

De OvJ wordt geadviseerd en op de hoogte gebracht van de bevindingen. De OvJ beslist of het lichaam wordt vrijgegeven of dat een opsporingsonderzoek gestart moet worden.

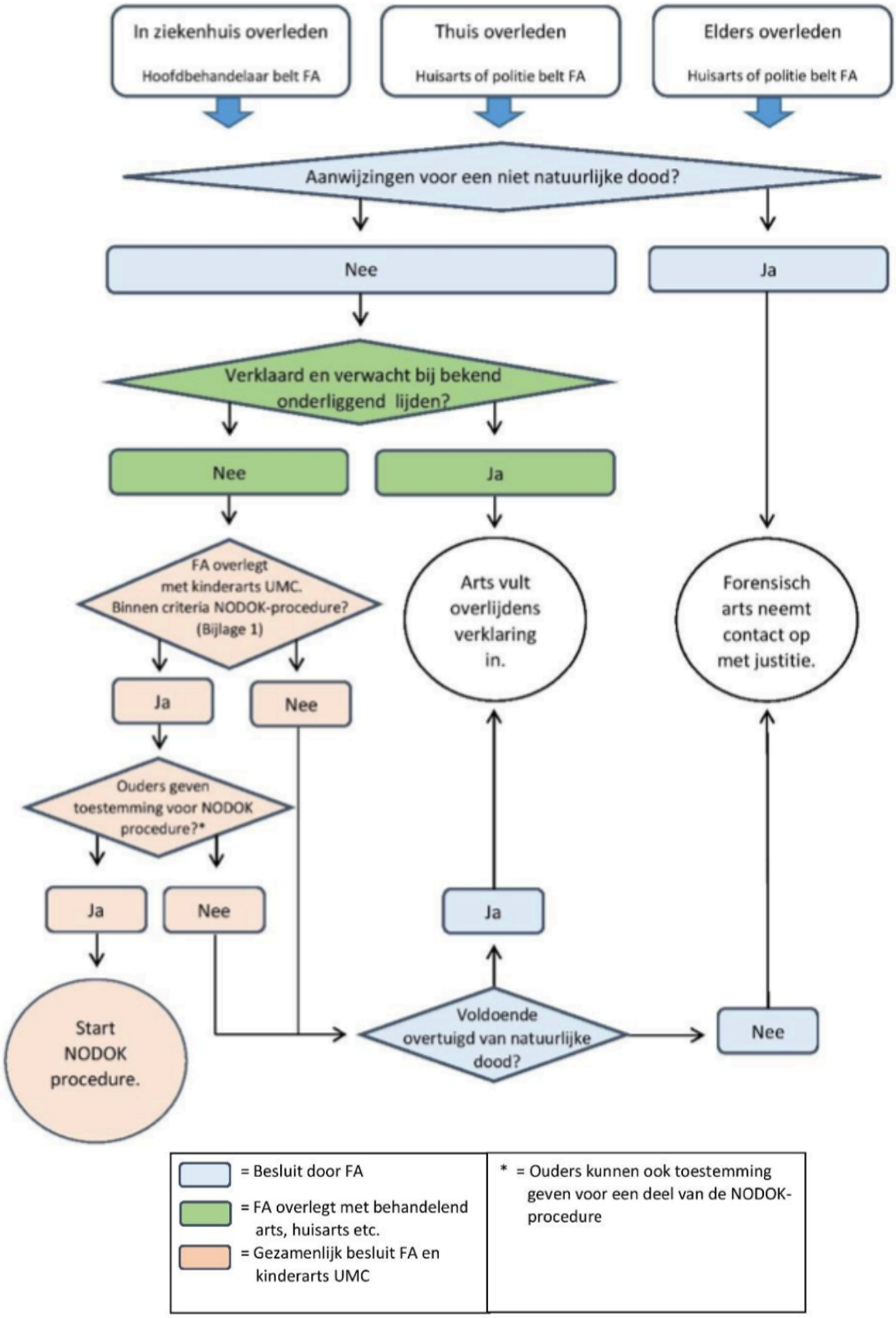
- *Niet overtuigd van natuurlijke dood en misdrijf kan niet uitgesloten worden*

De OvJ wordt geadviseerd en op de hoogte gebracht van de bevindingen. De OvJ beslist of het lichaam wordt vrijgegeven of dat een opsporingsonderzoek gestart moet worden.

- *Niet-natuurlijk overlijden met aanwijzingen van een misdrijf*

De arts adviseert samen met de tactische en de forensische recherche over het verrichten van een gerechtelijke sectie. De OvJ beslist of een opsporingsonderzoek gestart moet worden.[62]

Deze inzetcriteria gelden alleen voor overlijdensonderzoeken bij volwassenen.[3] Dascha Graafsma was 16 jaar. Bij een overlijden van een minderjarige wordt er pas contact gezocht met justitie wanneer de forensisch arts aanwijzingen van een niet-natuurlijk overlijden heeft geconstateerd.[63]
Als er volgens de forensisch arts geen aanwijzingen zijn voor een niet-natuurlijke dood, dan start de procedure ‘Nader onderzoek naar doodsoorzaak bij kinderen (NODOK) (zie figuur 1).[64] Deze procedure geeft ouders de mogelijkheid om de doodsoorzaak van hun kind vast te stellen. Naast het bijdragen aan preventie van overlijdensgevallen in de toekomst kan het ook helpen in de rouwverwerking.[64]



Figuur 1. *Het proces van het starten van de NODOK procedure.*[64]

Deze criteria zijn sinds 1 augustus 2016 van toepassing.[63] Dascha Graafsma was voor 1 augustus 2016 overleden.[4] Toen werden onverklaarde natuurlijke overlijdens nog onderzocht in een justitiële setting.[63]
Dascha is op 28 november 2015 om 05:20 uur in aanraking gekomen met een trein. De forensische en tactische opsporing en de forensisch arts zijn ter plekke gekomen, zoals dat zou moeten volgens de inzetcriteria.[3]

4.2 In beslag nemen van digitale gegevensdragers

Uit het interview met MTI komt naar voren dat de laptop van Dascha thuis lag. Deze is op 29 november 2016, een dag na het overlijden van Dascha, in beslag genomen door de politie. Art. 94 Sv. omschrijft in welke gevallen een voorwerp vatbaar kan zijn voor inbeslagname.[43] De laptop van Dascha is vatbaar voor inbeslagname omdat het de waarheid aan het licht kan brengen. Het in beslag nemen van een voorwerp is een dwangmiddel omdat het een inbreuk vormt op de rechten van de eigenaar van het voorwerp.[65] Volgens art. 96 Sv. is een opsporingsambtenaar bevoegd om voorwerpen in beslag te nemen als er sprake is van een verdenking van een misdrijf als omschreven in art. 67 eerste lid.[43] Er moet dus sprake zijn van een redelijk vermoeden, die op grond van feiten en omstandigheden moet worden vastgesteld.[66]

Bij een lijkvinding worden de vier basis-hypotheses opgesteld: moord, ongeval, natuurlijke dood, suïcide.[46] MTI is van mening dat het onderzoek sterk is beïnvloed door de verklaring van de machinist. De machinist verklaarde dat hij Dascha zag staan op het spoor en had hij twee keer geclaxonneerd, maar Dascha bleef staan en keek in de richting van de trein.[2] De verklaring van de machinist steunt de hypothese suïcide, aangezien Dascha de trein zag aankomen en bleef staan. De FO trof Dascha aan zonder bovenkleding. Het is onduidelijk of zij voor de aanrijding bovenkleding droeg omdat de machinist zich dit niet kan herinneren.[2] De bevindingen van de forensisch arts steunen de hypothese suïcide. De forensische en tactische opsporing en forensisch arts concludeerden samen dat er sprake was van suïcide. De OvJ werd geadviseerd en besloot om het lichaam vrij te geven.

De familie werd die dag op de hoogte gebracht van de bevindingen van het onderzoek.[3] De familie en vrienden geloven niet dat Dascha suïcide heeft gepleegd omdat ze overkwam als een blij en gelukkig persoon. De vriendinnen van Dascha verklaarden dat ze die nacht naar het 16+ feestje bij Let's Get Down in Hilversum zijn gegaan. Rond 02:00 uur zei Dascha tegen haar vriendinnen "dat ze even ging plassen". Dit was de laatste keer dat de vriendinnen haar hebben gezien. De politie heeft camerabeelden opgevraagd en hieruit is te zien dat Dascha rond 02:00 uur via de nooduitgang het feest heeft verlaten.[3] Op basis van deze bevindingen kan de hypothese misdrijf niet worden uitgesloten en kan er sprake zijn van een verdenking van een misdrijf zoals omschreven in art. 67 lid 1 en is de opsporingsambtenaar krachtens art. 96a Sv. bevoegd om de laptop in beslag te nemen. Het is opmerkelijk dat er in eerste instantie is uitgegaan van suïcide, maar dat de verklaringen van de familie en vrienden aanleiding gaven voor onderzoek. Dit toont aan dat het belangrijk is dat de politie verder kijkt dan alleen de plaats delict.

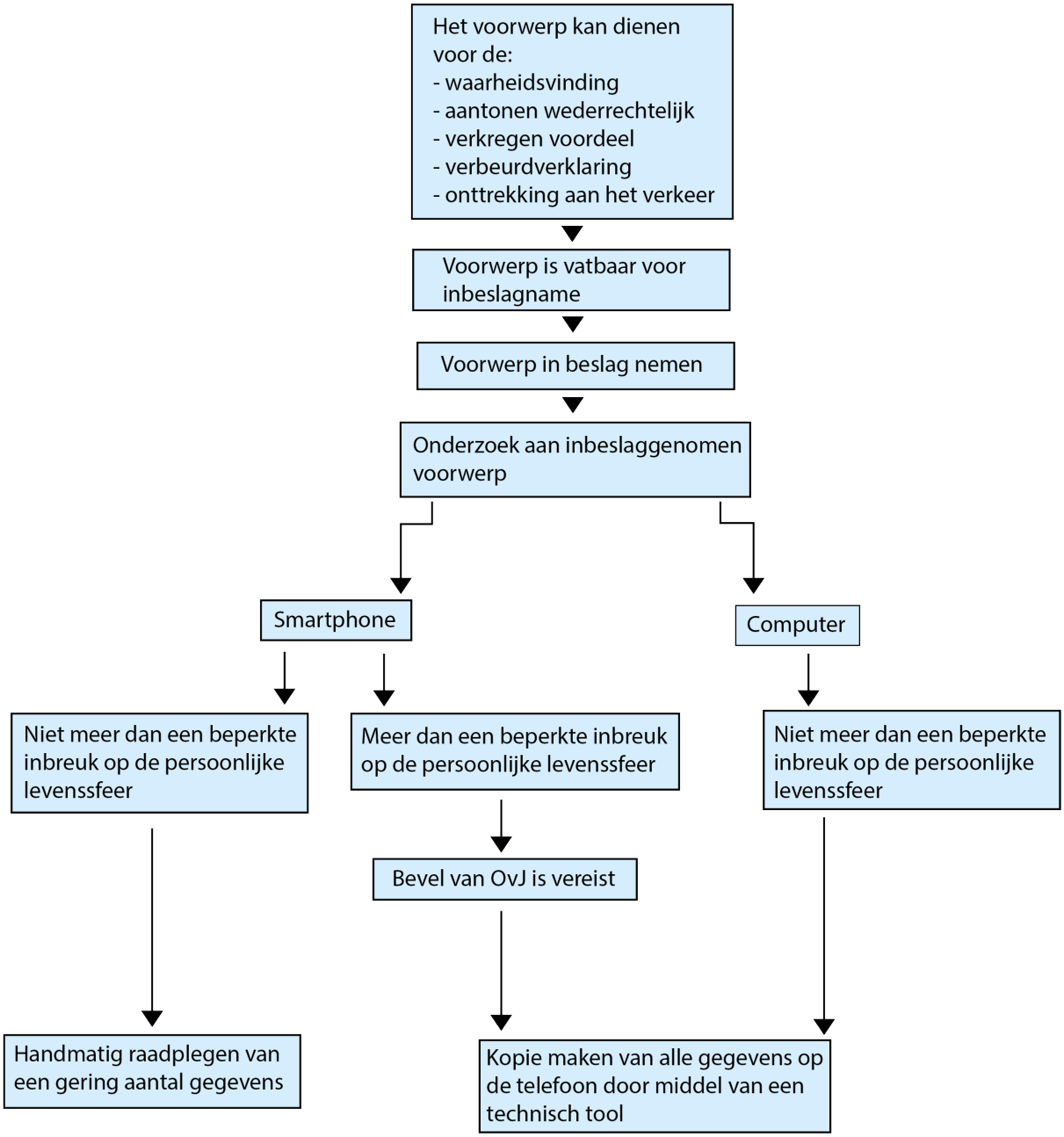
De laptop van Dascha lag thuis.[2] Art. 9b Sv. stelt dat een opsporingsambtenaar toestemming nodig heeft om de woning te betreden om vervolgens de laptop in beslag te nemen. Zonder toestemming is een schriftelijke machtiging tot binnentreden nodig. De machtiging kan verstrekt worden door de advocaat generaal of de (hulp)OvJ.[7]

Tot zover het in beslag nemen van de laptop van Dascha. De politie heeft rond 30 november 2015 onderzoek verricht aan de laptop. Onderzoek aan een in beslag genomen voorwerp is toegestaan voor de waarheidsvinding, computers zijn hiervan niet uitgezonderd. Art. 94 Sv. biedt hiervoor voldoende grondslag.[50] MTI is van mening dat de politie standaard een rapport maakt, maar er geen analyse meegedaan wordt. Volgens de politie was er een "zelfdoding" bestand aangetroffen in de laptop van Dascha. Later kwamen de nabestaanden erachter dat dit een pdf-bestand was van een schoolboek van Dascha dat ging over de zelfdoding van Hitler. Een opsporingsambtenaar mag onderzoek verrichten aan de laptop zolang er geen min of meer compleet beeld wordt verkregen van bepaalde aspecten van het persoonlijk leven van de gebruiker van de gegevensdragers.

In het rapport van MTI wordt verwezen naar een brief van de OvJ.[2] De brief geeft een beeld van het uitgevoerde politieonderzoek. Op 28 november 2015 is het onderzoek naar aanleiding van het onderzoek op de plaats delict, gesloten. Omdat de familie vragen had over de toedracht van het overlijden is het onderzoek heropend en is onder andere de laptop van Dascha onderzocht. Volgens de OvJ bleek uit het onderzoek dat er geen aanwijzingen waren voor een misdrijf en daarom werd het onderzoek, in december 2015, voor de tweede keer gesloten. Zoals eerder besproken kunnen ouders door de NODOK-procedure toestemming geven om aanvullend onderzoek uit te voeren. Maar deze procedure is alleen van toepassing bij een natuurlijk overlijden.[64] Een suïcide is geen natuurlijk overlijden. Bovendien is de NODOK-procedure alleen van toepassing om de doodsoorzaak te achterhalen. De nabestaanden willen de toedracht van het overlijden achterhalen en niet de doodsoorzaak.

Op 6 januari 2016 werd de telefoon van Dascha, een iPhone 5s, aangetroffen door twee kinderen op een speelplaats. In het rapport van MTI komt naar voren dat de OvJ een aantal extra onderzoekshandelingen heeft laten verrichten op verzoek van de nabestaanden. Het is niet duidelijk in welke gevallen de OvJ ingaat op dit soort verzoeken. De politie heeft met behulp van UFED onderzoek verricht aan de telefoon. In het theoretisch kader is besproken dat de Hoge Raad heeft bepaald dat op het moment dat er gebruik gemaakt wordt van een technisch tool om een smartphone te onderzoeken, er een meer dan beperkte inbreuk gemaakt wordt op de persoonlijke levenssfeer.[53] Dit komt omdat de technologie zich zo heeft ontwikkeld dat mensen hun leven meedragen in hun smartphone. Door onderzoek te verrichten aan een smartphone is het daarom mogelijk om een min of meer compleet beeld te verkrijgen van bepaalde aspecten van het persoonlijk leven van de gebruiker van de smartphone.

Een overzicht van de bevoegdheden van opsporingsambtenaren in het kader van onderzoek aan inbeslaggenomen digitale gegevensdragers wordt weergegeven in figuur 2.



Figuur 2. *Onderzoek aan inbeslaggenomen voorwerpen.*

Maar deze regels zijn alleen van toepassing op het moment dat er sprake is van een verdenking van een strafbaar feit. Maar volgens de OvJ waren er geen aanwijzingen voor een strafbaar feit en moet er dus niet meer gehandeld worden volgens de strafvordering.[3] De nabestaanden willen dat er onderzoek wordt verricht aan de telefoon. Een dwangmiddel als inbeslagname omschreven in art. 96 Sv is niet nodig omdat er sprake is van vrijwillige medewerking.[65] Maar zonder het in beslag nemen van een voorwerp mag de politie er geen onderzoek aan doen omdat het voorwerp dan nog in bezit is van de rechtmatige eigenaar.

Maar hoe kon de OvJ toch beslissen om onderzoek te doen aan de telefoon als er geen sprake was van een strafvorderlijk belang? Een vergelijkbare situatie werd in 2019 ter discussie gesteld. De vraag daarbij was of het mogelijk is om standaard bloedonderzoek uit te voeren na een verkeersongeval waarbij alle betrokkenen zijn overleden.[68] Nabestaanden hebben er belang bij om te weten of de bestuurders eventueel alcohol- of drugs hebben gebruikt. Maar bloedonderzoek vormt een inbreuk op de onaantastbaarheid van het lichaam. Het recht op de onaantastbaarheid van het lichaam blijft gelden na de dood. Inbreuk op dit recht is alleen mogelijk als dit van belang is voor de strafvordering.[68]

Uit het bovenstaande komt naar voren dat er sprake moet zijn van een strafvorderlijk belang als er inbreuk gemaakt wordt op een recht. Onderzoek aan een smartphone kan inbreuk maken op het recht op privacy. Volgens de grondwetsgeschiedenis blijft artikel 10 van de grondwet, het recht op privacy, gelden na de dood.[69] Volgens de AVG, worden persoonsgegevens in Nederland niet meer beschermd na de dood.[21] Maar de gegevens van de smartphone worden verwerkt in het kader van de uitvoering van een politietaak. Daarom is niet de AVG maar de Wpg van toepassing.
Een politiegegeven is volgens de Wpg: elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak.[58] Een persoonsgegeven is informatie over een identificeerbare natuurlijke persoon.[18] Een overleden persoon is geen natuurlijk persoon. De Wpg geeft niet aan hoe de politie om moet gaan met gegevens van een overleden persoon. Op het moment dat persoonsgegevens worden verwerkt in het kader van een strafvorderlijk onderzoek, worden deze strafvorderlijke gegevens genoemd. Maar volgens de Wet Justitiële strafvorderlijke gegevens kunnen gegevens van een overledene geen strafvorderlijke gegevens zijn omdat dit geen persoonsgegevens zijn.[59]

Zoals eerder vermeld kan een smartphone een beeld geven van bepaalde aspecten van het leven van de gebruiker. Een smartphone kan bijvoorbeeld aangeven met wie er voor het laatst gecommuniceerd is, wat de laatste bezochte webpagina's zijn en waar de telefoon is geweest. Het raadplegen van een gering aantal gegevens van een in beslag genomen smartphone is toegestaan. Maar in beslag name is alleen toegestaan bij een verdenking van een misdrijf. Als een opsporingsambtenaar onderzoek verricht aan een smartphone die niet in beslag is genomen dan zou de opsporingsambtenaar strikt gezien, op grond van art. 138 ab Sv., computervredebreuk plegen omdat de smartphone een geautomatiseerd werk is van een andere. Maar als de rechtmatige erfgenaam hiervoor toestemming geeft is het geen computervredebreuk. In beslag name is mogelijk als de hypothese misdrijf niet uitgesloten kan worden. Het is dan maar de vraag of de hypothese misdrijf definitief uitgesloten kan worden als de smartphone van een overledene beschikbaar is, maar niet is uitgelezen. Door een smartphone niet te onderzoeken is de kans groot dat er veel informatie wordt gemist.

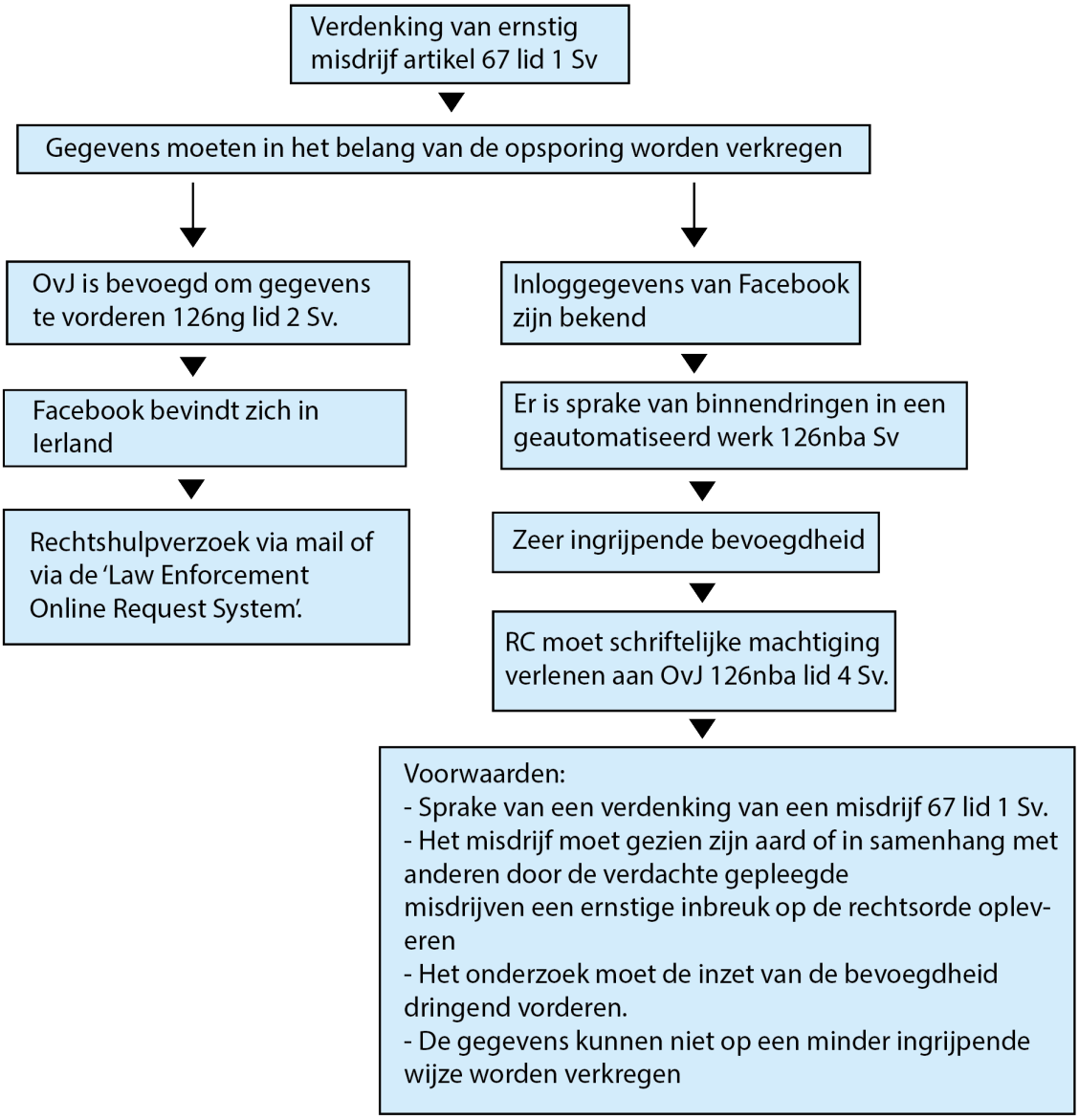
Binnen het opsporingsproces kan er alleen digitaal onderzoek worden verricht wanneer er sprake is van een verdenking van een strafbaar feit of een vermissing. Het is onduidelijk hoe er onderzoek verricht kan worden aan digitale gegevensdragers van overledenen op het moment dat uit het vooronderzoek blijkt dat er geen aanwijzingen zijn van een strafbaar feit. Dit omdat het niet bekend is of er inbreuk gemaakt wordt op de rechten van een overledene op het moment dat gegevens van een overledene geraadpleegd worden. Bovendien kan de digitale gegevensdrager ook gegevens bevatten van derden.

4.3 Social media

In het interview met Remon Verkerk kwam naar voren dat de politie vaak de inhoud van een social media account niet veiligstelt. In het rapport van MTI wordt een Facebook bericht besproken. Dit zou de politie volgens MTI verkregen hebben via het UFED rapport. Volgens de digitale specialist van i-Finish is het mogelijk dat UFED bepaalde Facebook notificaties extraheert omdat de telefoon deze informatie voor een bepaalde tijd opslaat. Volgens de nabestaanden waren de inloggegevens van het Facebook account van Dascha opgeslagen op de webbrowser van haar laptop. Het is van belang om te bepalen wat opsporingsambtenaren mogen doen met bekende inloggegevens.

De wet voorziet (nog) niet in de bevoegdheid om in te loggen op accounts. In januari 2019 heeft de Rechter Commissaris (RC) door tussenkomst van de OvJ opdracht gegeven aan een digitaal rechercheur om in te loggen in accounts van de verdachte om vervolgens de inhoud veilig te stellen.[70] De rechter-commissaris is op grond van art. 181 sv. bevoegd om deze vordering toe te wijzen. De rechter-commissaris verwijst naar artikel 126ng lid 2 Sv: *bij een verdenking van een misdrijf als omschreven in art. 67 lid 1 Sv, kan de OvJ, indien het belang van het onderzoek dit dringend vordert, de aanbieder van de dienst gegevens vorderen.* Om dit te doen moet een OvJ eerst een vordering doen aan de RC. Maar bij deze verordening worden er geen gegevens opgevraagd, maar logt de opsporingsambtenaar zelf in. De rechter-commissaris beargumenteert dat het inloggen in online accounts met beschikbare accountgegevens een wijze is van binnendringen in een geautomatiseerd werk. De wijze van binnendringen is eenvoudig en weinig risicovol (subsidiariteitsbeginsel). Het aanvragen van gegevens bij de aanbieder zou dezelfde inbreuk maken als het inloggen en veiligstellen van gegevens (proportionaliteitsbeginsel).[70]

Facebook bevindt zich in Ierland. Ierland is deel van het Cybercrime verdrag.[7] Nederlandse opsporingsambtenaren zijn op grond van artikel 32 van het Cybercrime verdrag bevoegd toegang te verschaffen tot bronnen die voor het publiek toegankelijk zijn. Een Facebookpagina is in het algemeen voor het publiek toegankelijk. Een Facebook gebruiker kan dit beperken door zijn of haar privacy-instellingen aan te passen.[71] Het zijn juist de gegevens die niet voor het publiek toegankelijk zijn, die vaak interessant zijn voor de opsporing.[72] Het kan voorkomen dat een opsporingsambtenaar onderzoek doet aan inbeslaggenomen digitale gegevensdragers en dat hij of zij de Facebook app tegenkomt waarmee er toegang gekregen kan worden tot een Facebook account. Dit is geen publiek toegankelijke bron, dus mag de opsporingsambtenaar geen onderzoek doen op de Facebookapplicatie. In het belang van de opsporing is het wel mogelijk om die gegevens te verkrijgen. Dit kan op twee manieren: door de communicatiedienst te vorderen om deze gegevens te verstrekken of door zelf in te loggen in het account. Er wordt verwezen naar figuur 3.



Figuur 3. *Overzicht van het verschil tussen gegevens van Facebook opvragen en zelf inloggen op het Facebook account.*

Nederland kan Facebook vorderen om bepaalde gegevens te verstrekken. Dit wordt gedaan via een internationale rechtshulpverzoek.[7] Hierbij wordt Facebook verzocht om gegevens te verstrekken in het kader van de opsporing. Bij politiële rechtshulp wordt er gevraagd voor het verkrijgen van informatie zonder enig gebruik te maken van dwangmiddelen. Deze informatie kan niet gebruikt worden als bewijsmateriaal in een rechtszaak. Dit mag wel bij een justitiële rechtshulp. Daarbij wordt de informatie verkregen van bevoegde justitiële autoriteiten door dwangmiddelen toe te passen, onderzoekshandelingen te verrichten of medewerking te verlenen.[73]

Het nadeel van een rechtshulpverzoek is dat het maanden kan duren voordat de aanvraag afgewikkeld wordt. Door zelf in te loggen kunnen de gegevens direct veiliggesteld worden. De RC noemt het inloggen in een account een vorm van binnendringen in een geautomatiseerd werk.[70] Dit is een zeer ingrijpende bevoegdheid. De wijze van binnendringen is op het eerste oog eenvoudig en weinig risicovol, maar er moet eerst achterhaald worden of de Facebookgegevens op een Nederlandse server staan. Als de locatie onbekend blijft of als de gegevens in het buitenland staan, biedt de wet de mogelijkheid om alsnog binnen te treden als dit noodzakelijk is.[54] De OvJ moet het belang van het onderzoek afwegen tegen de mogelijke schending van de soevereiniteit van een ander land.[7] Aangezien de bevindingen van het onderzoek aan de laptop en mobiel van Dascha geen aanleiding geven om extra gegevens van Facebook veilig te stellen, is het zeer waarschijnlijk dat het belang van de soevereiniteit veel zwaarder weegt dan het belang van het onderzoek.

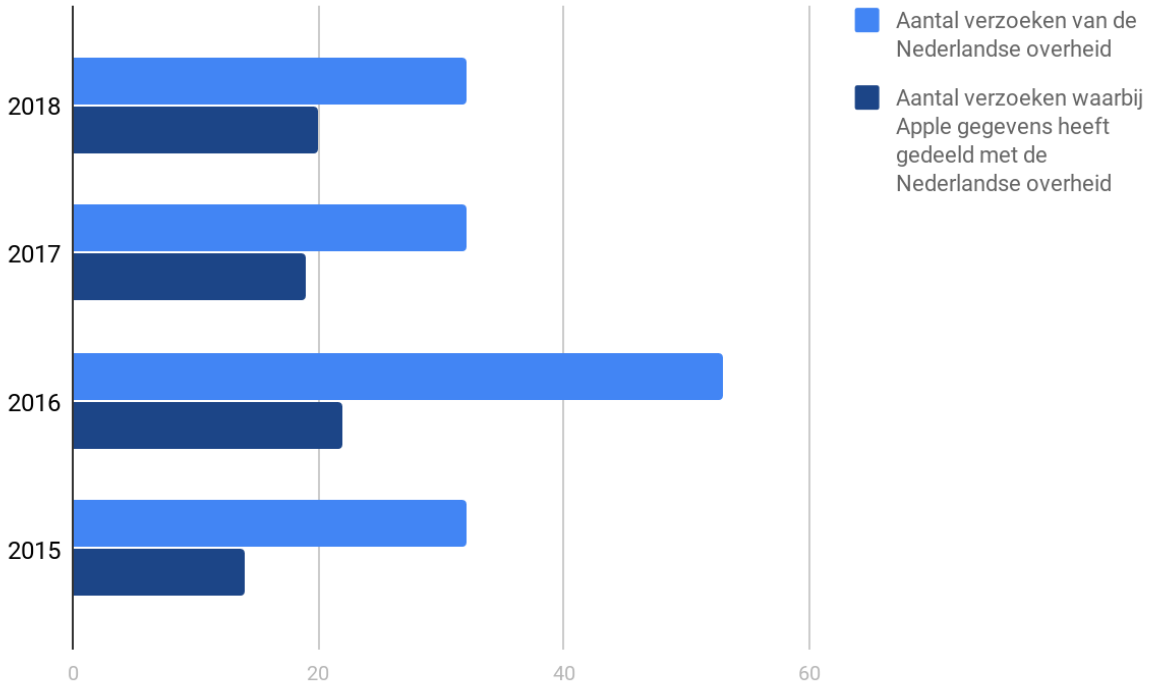
Volgens de OvJ bleek uit het politieonderzoek dat er geen aanwijzingen waren van een strafbaar feit. Het vorderen van Facebookgegevens via een rechtshulpverzoek is alleen toegestaan als er sprake is van een verdenking van een misdrijf. Het inloggen in een Facebook account van Dascha is, zonder toestemming van Facebook, een vorm van binnendringen in een geautomatiseerd werk.[44,7] Binnendringen is alleen toegestaan als er sprake is van een strafrechtelijk belang.

4.4 *Samenwerking met Facebook en Apple*

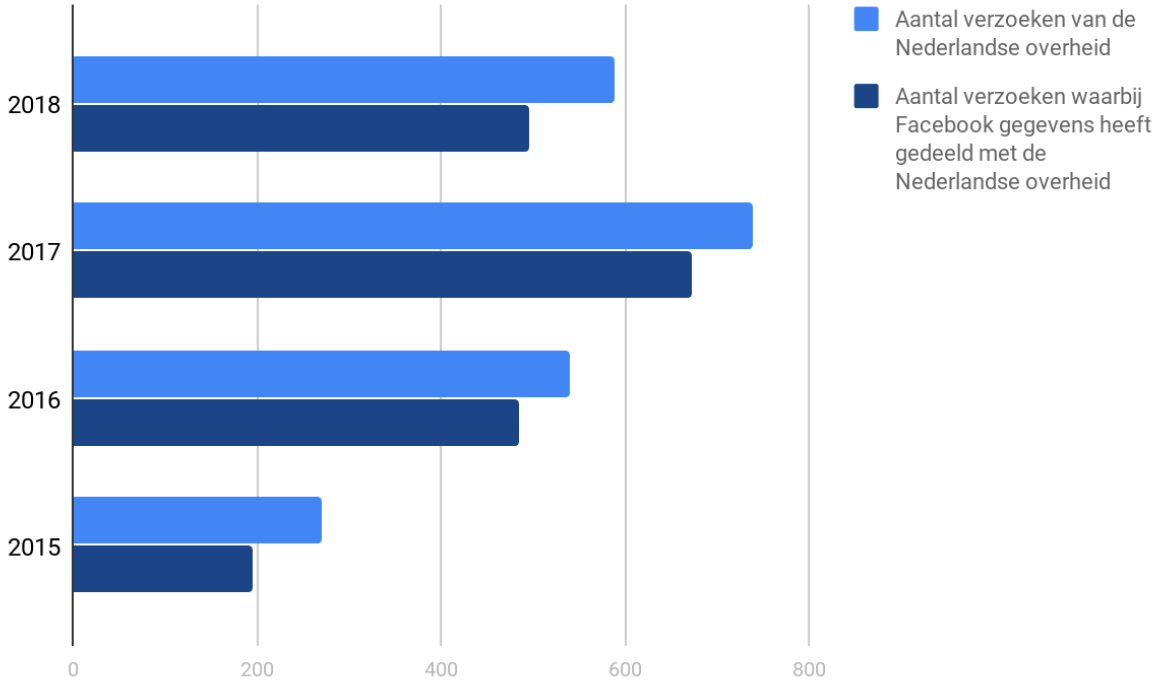
Er wordt opgemerkt dat het de politie is gelukt om data te extraheren uit de telefoon van Dascha. Uit het theoretisch kader blijkt dat Apple zijn apparatuur steeds beter beveiligt.[41] De opsporing kan gebruik maken van tools als Axiom Gray Key, om gegevens uit een Apple apparaat te extraheren.[16] In 2019 heeft de rechtbank bepaald dat er gebruik gemaakt mag worden van de vingerafdruk van een verdachte om toegang te krijgen tot een in beslag genomen smartphone.[74] Volgens de rechtbank is dit niet in strijd met het nemo-teneturbeginsel omdat een vingerafdruk materiaal is dat onafhankelijk van de wil van de verdachte bestaat. Door gebruik te maken van de vingerafdruk van een persoon wordt er een inbreuk gemaakt op de lichamelijke integriteit van de persoon.[74]

Zoals eerder besproken blijft dit recht gelden na de dood.[69] Een vingerafdruk van een overleden persoon, wanneer dit technisch mogelijk zou zijn, kan alleen gebruikt worden om een telefoon ontgrendelen als er sprake is van een strafvorderlijk belang.

Maar de politie kan ook de voor de opsporing relevante gegevens opvragen bij Apple.[41] Facebook en Apple publiceren elk half jaar transparency rapporten waarin wordt aangegeven hoe vaak de Nederlandse overheid een verzoek indient en hoe vaak de bedrijven de gegevens daadwerkelijk verschaffen. De transparency rapporten van Apple en Facebook zijn vergeleken (zie figuur 4 en 5).[75,76]



Figuur 4. *Aantal verzoeken van de Nederlandse overheid aan Apple van 2015 tot en met 2018.*



Figuur 5. *Aantal verzoeken van de Nederlandse overheid aan Facebook van 2015 tot en met 2018.*

Hieruit blijkt dat de Nederlandse overheid vaker verzoeken indient bij Facebook dan bij Apple. Bovendien verschaft Facebook vaker gegevens in vergelijking met Apple. Dit verschil kan verklaard worden doordat:

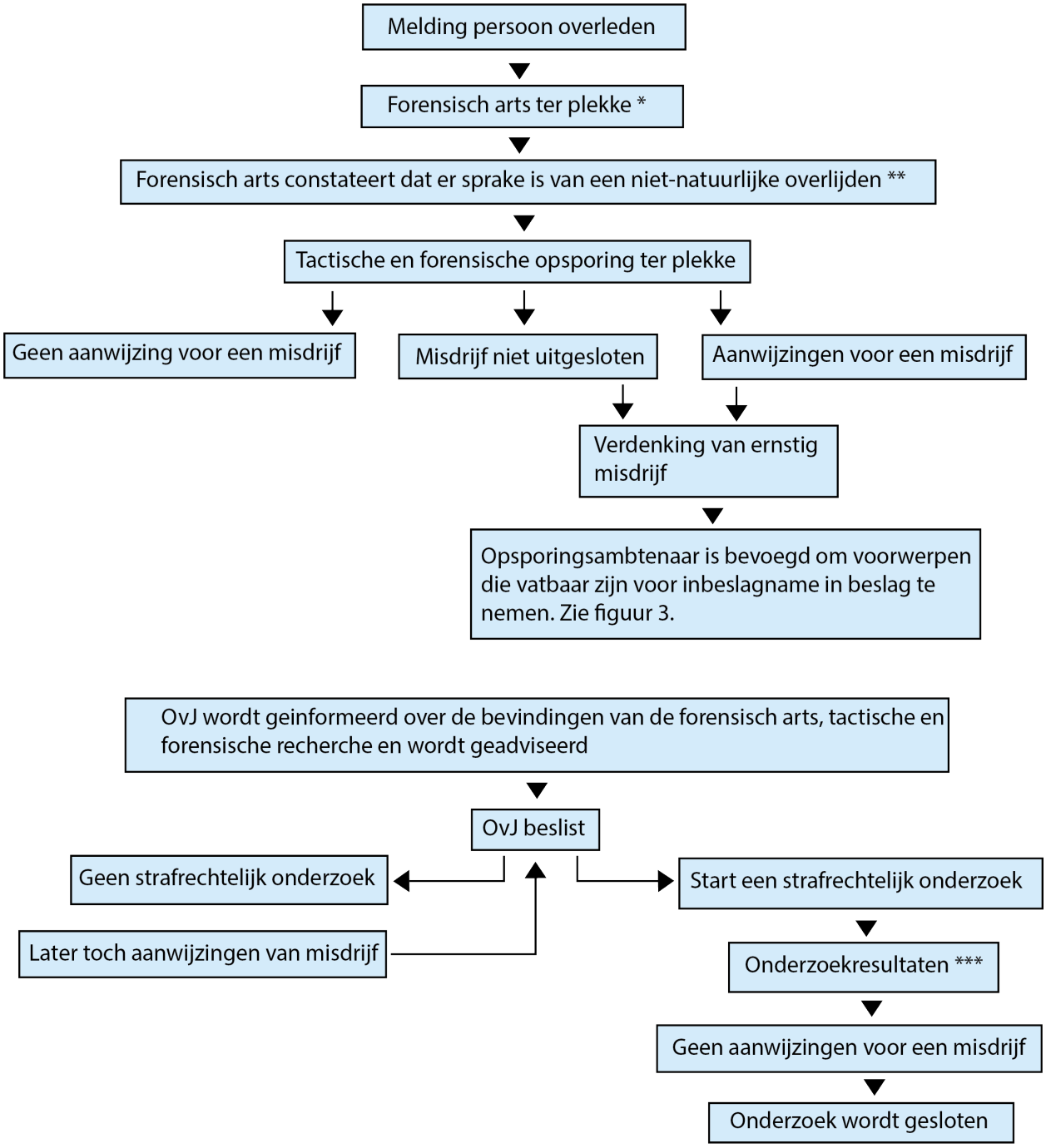
- doordat het voor Apple technisch gezien niet mogelijk is om deze gegevens te verschaffen en dit bekend is bij de Nederlandse politie of
- doordat de Nederlandse politie er geen belang bij heeft om de gegevens op te vragen.

De afwezigheid van dit belang kan als volgt verklaard worden.
Op het moment dat een digitale gegevensdrager in beslag is genomen mag deze onderzocht worden en mag er gebruik gemaakt worden van technische tools om toegang te krijgen tot de digitale gegevensdrager. Onderzoek aan een Facebook account, zonder toestemming van Facebook, is een vorm van heimelijk binnendringen in een geautomatiseerd werk en is alleen toegestaan onder strenge voorwaarden. Om toegang te krijgen tot Facebookgegevens moet de politie deze gegevens opvragen of toestemming vragen aan Facebook om de gegevens zelf veilig te stellen.[7] Samenwerking tussen Facebook en de Nederlandse politie is daarom essentieel.

Maar de transparency rapporten zijn gebaseerd op verzoeken vanuit de Nederlandse overheid. Het is onbekend hoeveel van deze verzoeken afkomstig zijn van de Nederlandse politie. Bovendien is het onbekend of de transparency rapporten gebaseerd zijn op officiële rechtshulpverzoeken of op basis van vrijwillige instemming.

4.5 *Het politieonderzoek sluiten*

Terugkomend op de zaak van Dascha. Op 30 november 2015 is een strafrechtelijk onderzoek gestart onder de hypothese dat iemand Dascha drugs heeft toegediend. De grondslag van dit onderzoek viel nadat bleek dat de NFI had geconcludeerd dat er geen drugs zijn aangetroffen in het lichaam van Dascha. Ook heeft de politie onderzoek aan het spoor gedaan, getuigen gesproken, camerabeelden en zendmastgegevens opgevraagd, onderzoek gedaan aan de laptop en mobiel, en toxicologisch onderzoek laten uitvoeren. Uit het politieonderzoek blijkt dat er geen aanwijzingen zijn van een strafbaar feit. De OvJ heeft de leiding in het onderzoek. Als de OvJ ervan overtuigd is dat er geen sprake is van een strafbaar feit, dan kan de OvJ het onderzoek sluiten.
De OvJ gaf aan dat het onderzoek “helaas geen uitsluitsel heeft kunnen geven over de vraag waarom Dascha op het spoor stond”. De OvJ is belast met het opsporen van strafbare feiten. De OvJ is niet belast met het opsporen van de toedracht van een suïcide, aangezien dit geen strafbaar feit is in Nederland. Een overzicht van dit proces wordt weergegeven in figuur 6 en 7.

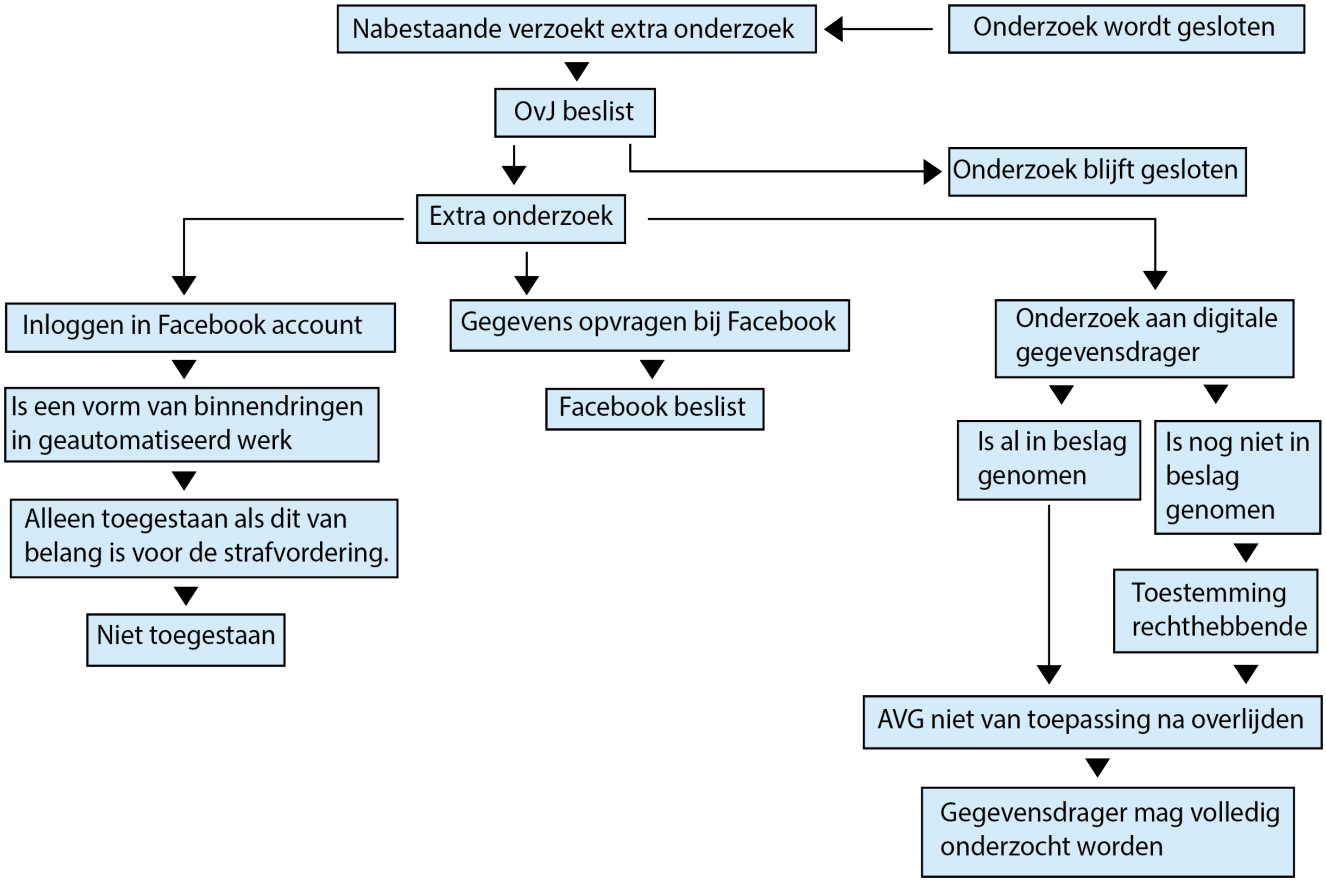


Figuur 6. *Overzicht van het opsporingsproces van melding tot het starten van een strafrechtelijk onderzoek*

*Het is mogelijk dat de tactische en forensische opsporing direct ter plekke komt als uit omstandigheden en feiten blijkt dat er sprake is van een niet-natuurlijk overlijden.

**En de reden van onderzoek geen medische fout of verklaard overlijden in een zorginstelling is.

***Tactische, forensische of medische onderzoeksresultaten.



Figuur 7. *Onderzoeksmogelijkheden als een nabestaande verzoekt om extra digitaal onderzoek te verrichten.*

De bevindingen van de politie worden gerapporteerd en toegevoegd aan het onderzoeksdossier. Nabestaanden kunnen een verzoek indienen bij de OvJ om het onderzoeksdossier in te zien. De Taskforce lijkschouw en gerechtelijke secties heeft in 2018 een rapport uitgebracht waarin wordt aangegeven hoe gegevens uit een onderzoek verstrekt kunnen worden aan de nabestaanden.[62] Daarbij is gevraagd aan de Tweede Kamer of het OM het onderzoeksdossier kan verstrekken aan nabestaanden. Daarop werd geantwoord dat dit per geval moet worden beoordeeld. De criteria van een afweging is toegevoegd aan het rapport. Hieruit blijkt dat verstrekking van gegevens die betrekking hebben op een overleden persoon mogelijk is zolang het onderzoek nog niet gesloten is of als er geconcludeerd is dat de doodsoorzaak niet duidelijk is.[62] Verstrekking kan dan toegestaan zijn ten behoefte van:

- rouwverwerking
- klacht op grond van art. 12 Sv.
- klacht over opsporingsambtenaren
- verzoek tot review
- verzoek tot aanvullende opsporingshandelingen

Dit moet per geval beoordeeld worden door de OvJ. De OvJ moet daarbij bepalen welk belang zwaarder weegt: het belang van inzage ten behoeve van rouw-of traumaverwerking of de privacybelangen van anderen.[59] Omdat de gegevens van een overleden persoon geen persoonsgegevens zijn biedt de wet geen grondslag voor het verstrekken van deze gegevens. De nabestaanden zijn daarom afhankelijk van de beslissing van de OvJ.

Volgens Remon Verkerk is de politie heel terughoudend met het delen van dit soort gegevens. In zijn ervaring gebeurt dit alleen bij het starten van een artikel 12 procedure. Als de OvJ besluit een zaak niet te vervolgen, dan kunnen belanghebbenden een artikel 12 procedure starten. Dit is een klacht tot niet-vervolging.[77] De dossiers worden dan alleen gedeeld met de advocaat van de nabestaanden. De advocaat is dan ook terughoudend in het delen van informatie met de nabestaanden.

De nabestaanden van Dascha mochten na drie jaar moeite het dossier inzien, maar niet meenemen.[3] Volgens de OvJ waren er geen verdachten voorgekomen in het onderzoek. De artikel 12 procedure is daarom niet van toepassing op deze zaak. De nabestaanden zijn het niet eens met de conclusie van de politie, en starten hun eigen onderzoek.

4.6 *De nabestaanden en de laptop van Dascha*

Nadat het politieonderzoek is gesloten is de laptop teruggegeven aan de familie. Art. 116 Sv. luidt dat de hulp-OvJ en de OvJ besluiten of het voorwerp nog van belang is voor de strafvordering.[43] Als het belang er niet meer is, dan wordt het voorwerp teruggegeven aan de persoon van wie het voorwerp in beslag is genomen. Het wachtwoord van de laptop was bekend bij de familie en deze werd doorgegeven aan MTI. Er wordt stilgestaan bij de vraag of de familie en MTI gebruik mogen maken van het wachtwoord. De wet stelt dat het strafbaar is om binnen te dringen in een geautomatiseerd werk van een ander. Maar op het moment dat iemand overlijdt, worden al zijn of haar vermogen overgedragen aan de rechtmatige erfgenaam. Een laptop is een deel van het vermogen.[78] De laptop wordt dus geërfd door de rechtmatige erfgenaam. Deze persoon is dan ook bevoegd om gebruik te maken van de laptop. Het is onbekend hoe de familie het wachtwoord weet. Maar omdat de erfgenaam de eigenaar is van de laptop is er geen sprake van “binnendringen in een geautomatiseerd werk van een ander” op het moment dat het wachtwoord wordt gebruikt. MTI heeft toestemming gekregen van de rechtmatige erfgenaam om te kijken in de laptop van Dascha. Dit om te achterhalen of er gegevens in staan die iets kunnen vertellen over de toedracht van haar overlijden. Op de webbrowser van de laptop waren wachtwoorden opgeslagen van onder andere social media accounts. Het is voor dit onderzoek van belang om te achterhalen waar de grens ligt op het moment dat iemand kijkt in de in de laptop van een overledene. Uit het bovenstaande wordt duidelijk dat met toestemming van de rechtmatige erfgenaam, MTI mag kijken in de laptop. Maar dit geldt alleen voor de gegevens die lokaal staan opgeslagen in de laptop. Op het moment dat er via die laptop ingelogd wordt op een online dienst, dan gelden de algemene voorwaarden van die dienst.[28]

4.7 *Facebook tegen de nabestaanden*

In de algemene voorwaarden van Facebook wordt gesteld dat het niet toegestaan is om:

- inloggegevens van het account te delen met anderen
- anderen toegang te geven tot het account
- het account over te dragen aan anderen

zonder toestemming van Facebook.[29]
Bij het helpcentrum van Facebook wordt aangegeven dat het altijd in strijd is met het Facebook beleid om in te loggen in het account van een ander.

In het interview werd MTI gevraagd hoe zij hiernaar kijken.
"Algemeen gezien vind ik dat je niet zomaar in een Facebook account van ander kan. Dit is een ander geval en er was al ingelogd op haar laptop. En wij hadden toestemming van haar familie. Dan zie ik het probleem niet zo. Kijk, op het moment dat die persoon leeft dan is het een heel ander verhaal natuurlijk."

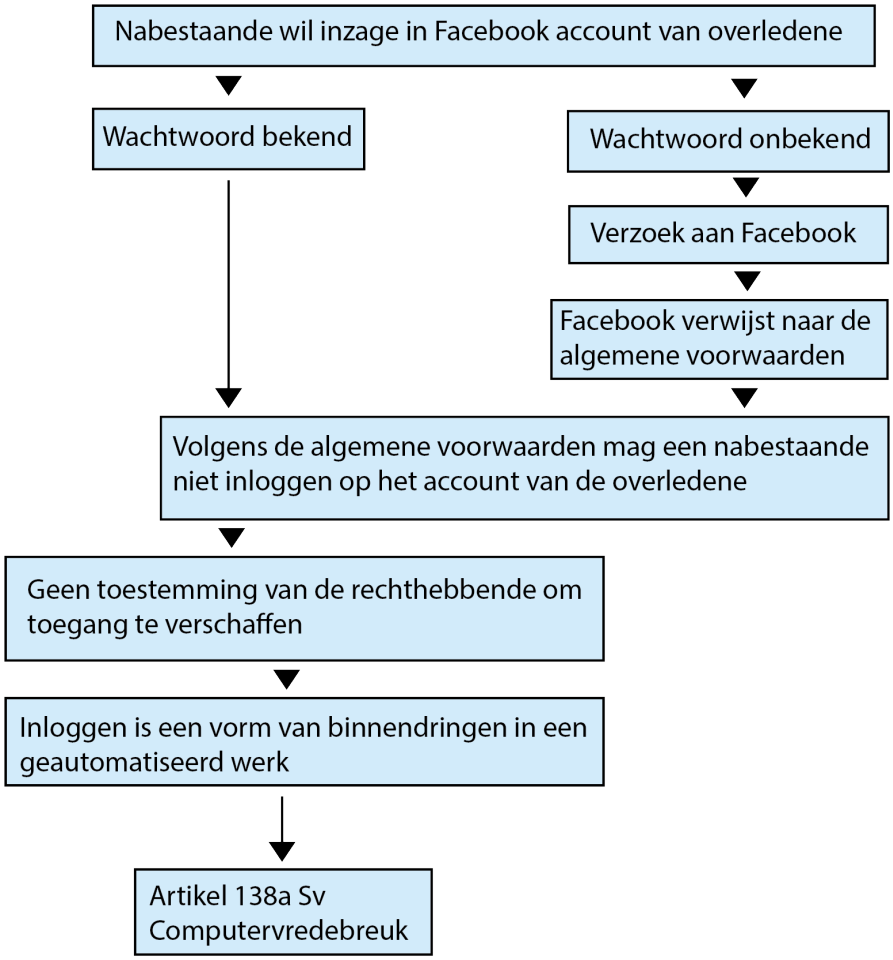
De toestemming van de familie geeft MTI geen recht om in het Facebook account te kijken. Dit omdat een Facebook account niet overdraagbaar is. Dascha heeft waarschijnlijk tijdens leven toestemming gegeven aan de webbrowser om haar Facebook accountgegevens op te slaan. Gezien het feit dat er al ingelogd was op haar laptop heeft MTI strikt gezien niet zelf handmatig ingelogd op het account.
Zoals eerder vermeld is het strafbaar is om binnen te dringen in een geautomatiseerd werk van een ander. Het Facebook account van Dascha is een geautomatiseerd werk van Dascha.[7] Art. 138ab Sr. geeft een beperkte definitie voor "binnendringen". Het is aan de rechter om per situatie vast te stellen of er sprake is van "binnendringen" in de zin van art. 138ab Sr.[79]

Er wordt gekeken naar eerdere uitspraken van de rechter. In 2018 gaf de rechter aan dat als iemand zich tegen de *onmiskenbare wil van de rechthebbende* toegang verschaft tot een geautomatiseerd werk, er sprake kan zijn van wederrechtelijk binnendringen.[80] De vraag is dan wie de rechthebbende van het Facebook account is. De gebruiker van het account is overleden en het account is niet overdraagbaar. Facebook wil niet dat iemand anders in het account inlogt. Dit maakt Facebook *onmiskenbaar* door dit te vermelden in de algemene voorwaarden. Verder gaf de rechter aan dat er sprake moet zijn van een *kenbare drempel* zodat anderen weten dat ze niet bevoegd zijn om zichzelf toegang te verschaffen. Als iemand naar www.facebook.com gaat en er is al ingelogd, dan is het niet heel duidelijk in hoeverre er sprake is van een *kenbare drempel.* Het is echter wel vrij gemakkelijk te zien dat je bent ingelogd in een account van een ander en daarmee te beseffen dat je daar niet hoort te zijn. In 2019 oordeelde de rechter dat er sprake kan zijn van binnendringen wanneer *iemand zichzelf toegang verschaft door het aannemen van een valse hoedanigheid*.[81] Een valse hoedanigheid is het aannemen van de identiteit van een geautoriseerd persoon door gebruik te maken van hun identificatie. Door in te loggen in het account van Dascha wordt er gebruik gemaakt van een valse hoedanigheid.

In het interview met Remon Verkerk, is gevraagd hoe hij hier tegenaan kijkt.
"Ik denk dat (en dan spreek ik even voor mijzelf) als nabestaanden het wachtwoord hebben en zij door het inloggen, de voorwaarden van Facebook zouden overtreden, dan zou dat mij niet uitmaken. Als recherchebureau moeten wij ons ook net als iedereen aan de wet houden en dat doen wij ook. Maar ja, dat soort dingen. Dat vind ik meer een civiele gelegenheid. Ik vind dat ik de afweging niet kan maken. Ik denk dat het belang van de nabestaanden boven het belang van Facebook gaat."

Een afweging tussen het belang en de inbreuk, dat is het toetsen van de proportionaliteit. In 2013 bepaalde de rechtbank dat: *inbreuk op een geautomatiseerd werk zonder toestemming van de rechthebbende strafbaar is, tenzij er onder zeer bijzondere omstandigheden hogere belangen zijn die een dergelijke inbreuk in volle omvang kunnen rechtvaardigen*.[82] Het belang van de nabestaanden van Dascha is op het eerste oog

waarheidsvinding. Maar de waarheidsvinding is eigenlijk direct gekoppeld aan het belang van rouwverwerking.
De nabestaanden willen de waarheid aan het licht brengen omdat het niet weten van de waarheid in de weg staat van het rouwproces. Facebook heeft ook een belang. Facebook wil met hun algemene voorwaarden waarschijnlijk de privacy van zijn gebruikers beschermen. Het Facebook account van Dascha bevat niet alleen gegevens van Dascha. Het bevat ook gegevens met derden. Het is in Nederland (nog) niet voorgekomen dat een rechter heeft bepaald dat het belang van het rouwproces zwaarder weegt dan de inbreuk op de algemene voorwaarden van Facebook en daarmee een inbreuk op de privacy van derden. Het inloggen in een Facebook account van een overleden persoon, zonder toestemming van Facebook, is een vorm van computervredebreuk omdat er binnengedrongen wordt in een geautomatiseerd werk van een andere. Een overzicht van dit proces wordt weergegeven in figuur 8.



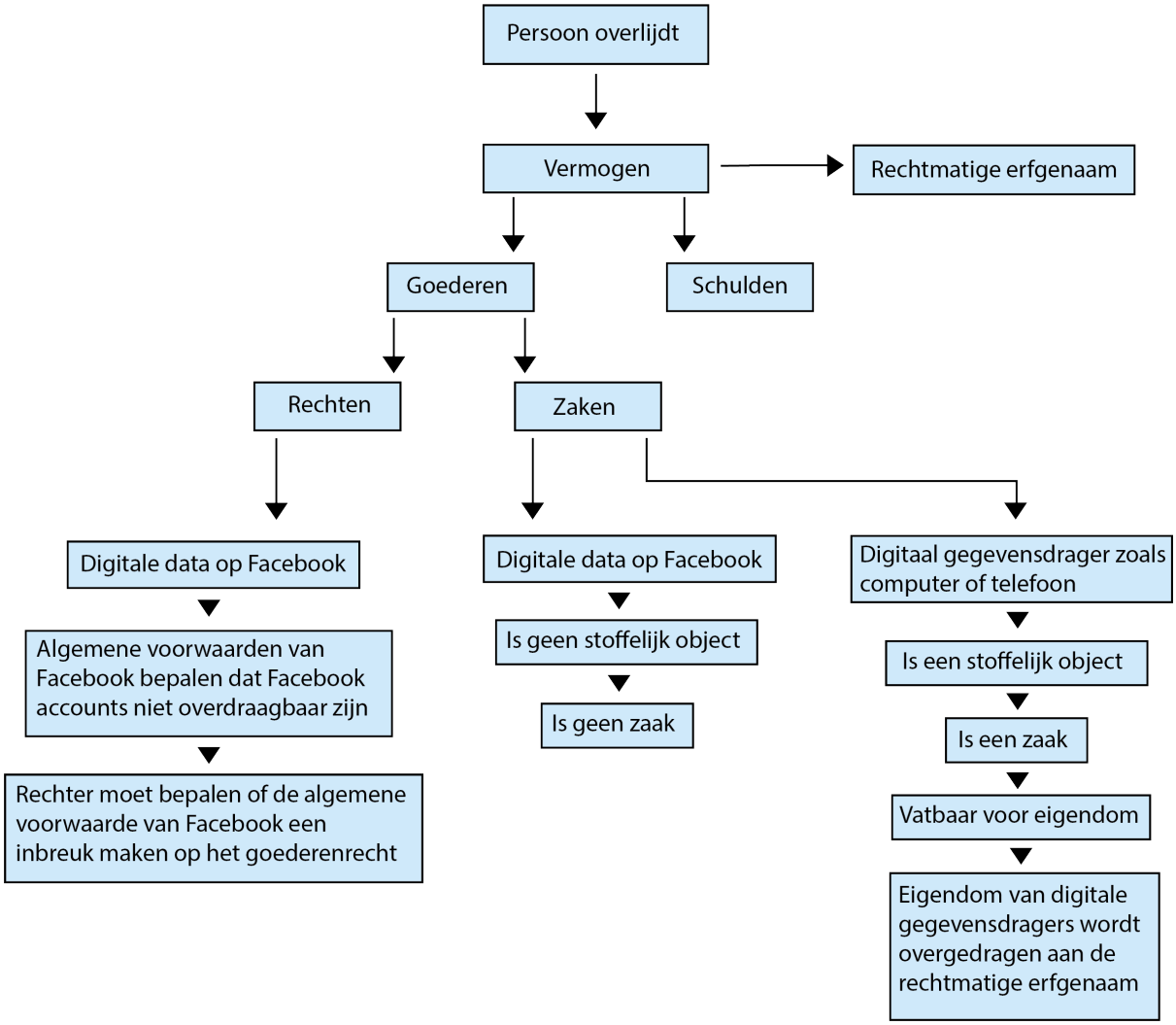
Figuur 8. *De rechten van een nabestaande rondom het Facebook account van een overledene.*

4.8 Het erfrecht

Er is een interview gehouden met de Koninklijke Notariële Beroepsorganisatie (KNB). De KNB is een organisatie die zich bezighoudt met het bewaken en bevorderen van de kwaliteit van het notariaat.[83] Uit het interview kwam naar voren dat het inderdaad zo is dat een rechtmatige erfgenaam de digitale gegevensdrager van de overledene erft. Maar wat er met de online accounts van de overledene gebeurt, is niet bekend. Een testament regelt de overgang van vermogens. Spaargeld, aandelen of woningen zijn voorbeelden van vermogens.
Naast een testament kan een persoon bepaalde wensen ook in een codicil laten vastleggen. Een codicil is, in vergelijking met een testament, geldig zonder tussenkomst van een notaris.[83] Een codicil moet dan wel handgeschreven en ondertekend zijn door de erflater. In een codicil kan een erflater bepalen wat er met zijn of haar roerende goederen moet gebeuren. Roerende goederen zijn goederen die verplaatsbaar zijn zoals auto's, sieraden en meubels.[84] Hiernaast kan een erflater duidelijk maken wat zijn wensen zijn.[85]

Kan een erflater ook in een codicil vastleggen wat er moet gebeuren met zijn data? Van wie zijn data eigenlijk?
Als gegevens leiden tot de identificatie van een persoon, is de AVG van toepassing. Iemand heeft dankzij de AVG het recht om alle gegevens van zichzelf op te vragen aan degene die zijn of haar gegevens verwerkt, zoals Facebook. Op het moment dat een persoon komt te overlijden, vervalt dit recht.[18]

Op het moment dat een persoon overlijdt wordt zijn of haar vermogen overgedragen aan de rechtmatige erfgenaam (zie figuur 9). Iemands vermogen bestaat uit goederen en schulden. Goederen zijn alle zaken en alle vermogensrechten.[86] Zaken zijn de voor menselijke beheersing vatbare stoffelijke objecten.[87] Een laptop of telefoon is een zaak en is daarom vatbaar voor eigendom. Data vormen geen zaken. Het is dan de vraag of data op onlineaccounts kunnen vallen onder vermogensrechten. Als data vallen onder het vermogensrecht dan wordt het overgedragen aan de rechtmatige erfgenaam. Maar de rechtmatige erfgenaam wordt beperkt door de contractuele bepaling tussen Facebook en de overleden persoon. Facebook geeft aan dat het account, in verband met privacyregels, niet overdraagbaar is. Als iets niet overdraagbaar is, kan het niet vallen onder het goederenrecht.



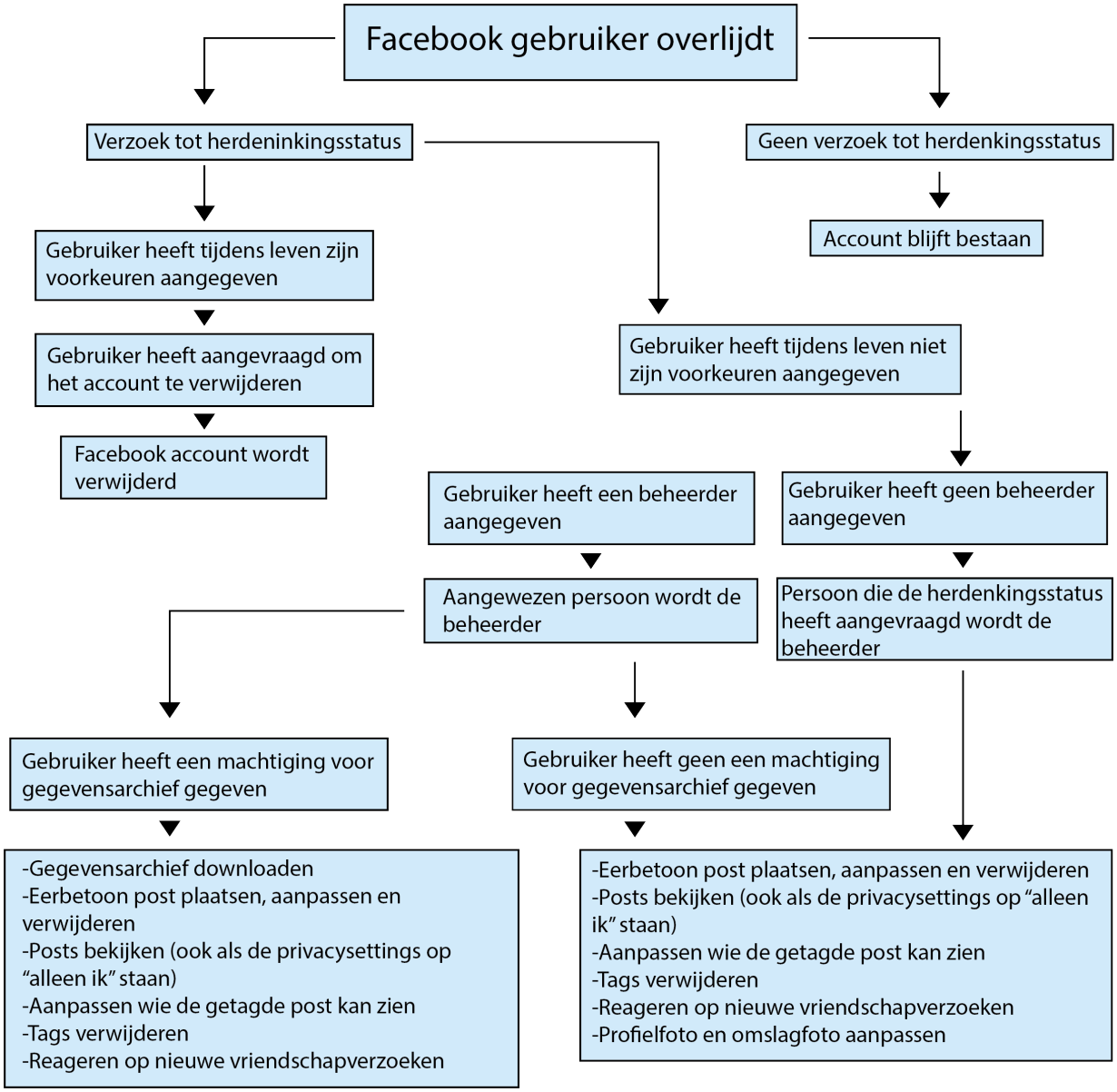
Figuur 9. Het erven van digitale gegevensdragers en de belemmering van de algemene voorwaarden van Facebook.

Of de algemene voorwaarden van Facebook een inbreuk maken op het goederenrecht moet een rechter bepalen. In Nederland is een dergelijke rechtszaak nog niet voorgekomen maar in Duitsland wel.

In 2015 vond er in Duitsland een rechtszaak plaats waarbij ouders aan Facebook verzochten om toegang te krijgen tot Facebook account van hun overleden dochter. Hun dochter was in 2012 geraakt door een trein in Berlijn. De ouders weten niet of het een zelfmoord of ongeluk was en hoopten dit te achterhalen door inzage te krijgen in haar Facebook berichten.[88]
De rechtbank kwam tot de conclusie dat een social media account en de inhoud ervan deel uitmaakt van de nalatenschap. Het contract tussen de gebruiker en de aanbieder moet overgedragen worden aan de nabestaanden.
Facebook ging 2016 in hoger beroep. Volgens Facebook kan digitale data niet op dezelfde manier behandeld worden als analoge informatie. Data is ongrijpbaar en kan niet fysiek tot iemand behoren. Data van Facebook wordt bovendien niet opgeslagen op een computer, maar op een server. Facebook verwees dan ook naar de privacy van derden. De rechtbank

gaf de ouders geen toegang tot het Facebook account en beargumenteerde dat het erfrecht niet in de mogelijkheid voorziet om toegang te krijgen tot die gegevens.
De rechter gaf aan dat, ook al had de dochter haar inloggegevens verstrekt aan haar moeder, het alsnog niet toegestaan is om hiervan gebruik te maken. De rechter heeft ook gekeken naar de vraag of een overeenkomst tussen een gebruiker van een online dienst en de aanbieder overgedragen moet worden aan de erfgenamen. De rechtbank kon dit niet beantwoorden en gaf de ouders toestemming om een speciaal beroep te doen op het Federale Hof van Justitie.[89] Het Hof oordeelde dat een contract overgedragen wordt aan de erfgenamen en daarmee hebben de erfgenamen het recht om toegang te verschaffen tot het account. Volgens het Hof moeten digitale gegevens niet anders behandeld worden dan analoge gegevens zoals bijvoorbeeld een dagboek.[89]

Dit arrest betekent niet dat rechtmatige erfgenamen automatisch toegang hebben tot Facebook accounts van overledenen. Facebook vraagt nog steeds eerst een gerechtelijk bevel. Verder biedt Facebook de optie aan om het account een herdenkingsstatus te geven. Wanneer de overledene tijdens leven geen beheerder heeft aangewezen, dan wordt de aanvrager de beheerder van het account met herdenkingsstatus.[90] Een schematische weergave dit proces wordt weergegeven in figuur 10.



Figuur 10. *De mogelijkheden die Facebook biedt na het overlijden van een gebruiker.*

Een nabestaande kan op deze manier inzage krijgen in nieuwe informatie zoals de nieuwe vriendschapsverzoeken en posts waarvan de privacy settings op "alleen ik" staan. Indien de gebruiker tijdens leven een machtiging heeft gegeven, dan kan de nabestaande deze gegevens downloaden. Er wordt geen inzage gekregen in foto's of video's waarvan de privacy settings op "alleen ik" zijn ingesteld, privéberichten, advertenties waar de gebruiker op heeft geklikt en pokes.[37] Het probleem is dat iedereen een memorial pagina kan aanvragen. Alleen bij het verwijderen van het account houdt Facebook rekening met verificatie van de persoon.

Bepaalde bedrijven en notarissen bieden erflaters aan om een ‘social media akte’ op te stellen. In deze akte kan een erflater kan vastleggen wat er met zijn of haar social media accounts moet gebeuren. Om de wensen ook daadwerkelijk uit te kunnen voeren, moet de erflater ook de bijbehorende inloggegevens laten vastleggen. Een ‘social media akte’ heeft geen waarde omdat het huidige erfrecht geen mogelijkheid biedt om social media accounts te erven. De algemene voorwaarden zijn bepalend. De algemene voorwaarden bepalen dat een rechtmatige erfgenaam niet mag inloggen in een account van de overledene, ook al was dat de wens van de wet en overledene. Nabestaanden worden door een ‘social media akte’ uitgelokt tot het plegen van computervredebreuk.

4.9 Apple tegen de nabestaanden

Tot zover de rechten van nabestaanden voor het gebruiken van een computer en toegang krijgen tot het Facebook account van de overledene. Het is voor dit onderzoek van belang om ook te kijken naar de mogelijkheden als nabestaanden niet beschikken over het wachtwoord van de laptop.

Uit het theoretisch kader blijkt dat Apple steeds streeft naar een betere beveiliging. Een Apple laptop die gebruik maakt van de Mac OS 10.3 of hoger maakt gebruik van FileVault.[91] Dit is een encryptie software die ervoor zorgt dat je zonder het wachtwoord de data niet kan zien. Het is dus niet mogelijk om de inhoud van de harde schijf te extraheren, omdat de data geëncrypt blijft zolang het correcte wachtwoord niet is ingetoetst.[92] Volgens i-Finish is het kraken van een wachtwoord afhankelijk van de moeilijkheidsgraad van het wachtwoord. Zo is een wachtwoord van drie letters makkelijker te kraken dan een wachtwoord van tien letters, waarvan een paar hoofdletters zijn, een paar cijfers en nog eens een paar leestekens. Verder zijn er ook andere technieken. Maar voor Apple computer apparatuur dat recent is uitgebracht, geldt dat het voor commerciële bedrijven steeds lastiger wordt om deze te kraken. Een nabestaande zou dan hulp kunnen vragen aan Apple. In een gehouden interview met een rechtmatige erfgenaam en als zodanig betrokken bij een suïcide, bleek de problematiek een reflectie te zijn van de eerder aangehaalde tientallen vragen die spelen bij nabestaanden.
Zo willen nabestaanden vaak primair toegang tot gegevens op apparatuur van de overleden voor de emotionele verwerking maar ook voor de noodzakelijke afwikkeling van zaken. Voorbeelden zijn dan om te kunnen beschikken over dierbare foto’s en films van de overledene als herinnering tot de zakelijke verplichting voor nabestaanden om aangifte te doen bij de belasting maar de te overleggen administratie daartoe staat (digitaal) op een computer of in de cloud met onbekende gebruikersnamen en wachtwoorden.

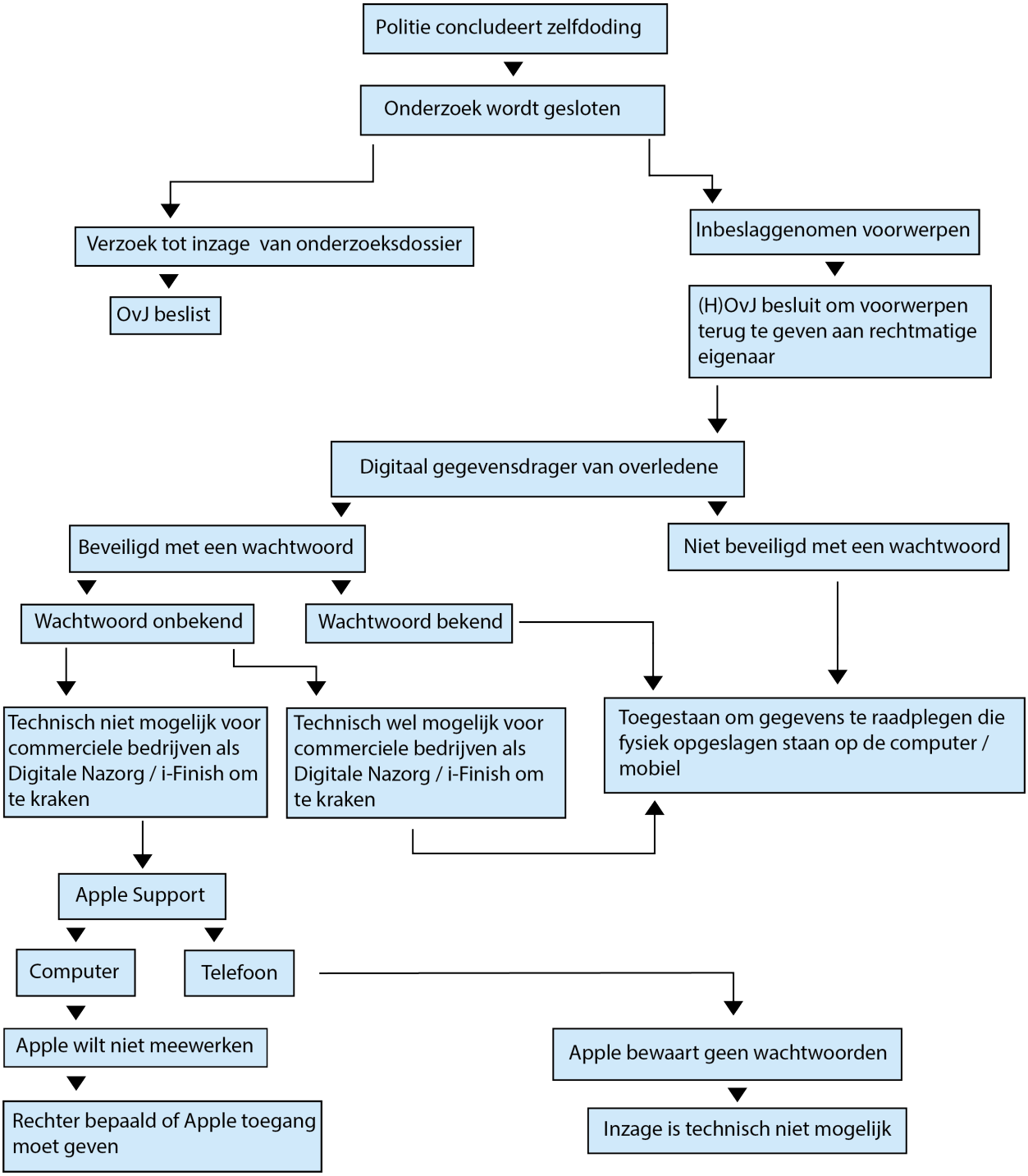
In vrijwel alle gevallen blijkt dat door nabestaanden eerst contact is gezocht met Apple Support Nederland, een tijdrovend en langdurig proces waarbij nabestaanden meerdere malen worden doorverwezen naar verschillende afdelingen en contactpersonen. Wanneer er al toezeggingen werden gedaan met betrekking tot (de inhoud van) accounts, werden deze bovendien nooit nagekomen.
Het bleek ook alleen mogelijk om telefonisch contact te hebben met Apple, waardoor de nabestaande nooit kon bewijzen dat bepaalde beloftes zijn gedaan. Contactpersonen van Apple gaven soms als laatste mogelijkheid aan dat de nabestaande via een gerechtelijk

bevel kon proberen toegang te krijgen tot Apple apparatuur. Er werd geen garantie gegeven dat dit ook zou lukken.

4.10 De nabestaanden en de telefoon van Dascha

Tot zover de mogelijkheden voor het verschaffen van toegang tot een laptop van een overleden persoon. Zoals eerder vermeld, is de telefoon van Dascha op 6 januari 2016 aangetroffen en in beslag genomen. De telefoon is door twee spelende kinderen aangetroffen. In art. 116 Sv. staat beschreven dat de persoon bij wie het voorwerp in beslag is genomen, afstand kan doen van het voorwerp.[43] Het voorwerp kan dan teruggegeven worden aan degene die redelijkerwijs als rechthebbende kan worden aangemerkt. De telefoon is ongeveer twee weken later aan de ouders van Dascha overhandigd.[3] Volgens MTI ging de telefoon niet aan. Dit komt waarschijnlijk omdat de telefoon waarschijnlijk meer dan een maand buiten gelegen had. Het is onbekend hoe het de politie is gelukt om data uit de telefoon te extraheren. Volgens MTI heeft de politie onderdelen toegevoegd aan de telefoon waardoor het is gelukt om de data eruit te extraheren. Toen de nabestaanden de telefoon terugkregen, ging de telefoon ook niet aan. Dascha heeft die bewuste avond nog een backup gemaakt van haar telefoon. Deze back-up stond fysiek opgeslagen op haar laptop. Deze back-up is geladen op een andere telefoon van hetzelfde model (iPhone 5s). De rechtmatige erfgenaam mag de back-up raadplegen omdat dit fysiek op de laptop staat. De nabestaanden van Dascha hebben het voordeel dat ze bekend waren met het wachtwoord van de laptop en dat er een back-up van de mobiel gevonden werd op de laptop. Het komt ook voor dat nabestaanden niet beschikken over deze informatie. In de vorige paragraaf is gekeken naar de mogelijkheden rondom een laptop van Apple. Er wordt nu gekeken naar telefoons van Apple.

Een toegangscode van een Apple telefoon wordt bewaard op de telefoon. Apple is daarom zelf niet bekend met de toegangscodes en kan dus geen toegang verkrijgen tot iPhones. Bovendien kan Apple geen data extraheren uit telefoons met een onbekende toestelcodes die gebruik maken van iOS 8.0 en nieuwere versies van de iOS software omdat deze software ervoor zorgt dat alle data encrypt is.[41] Apple geeft aan dat zij niet beschikken over de sleutel om de data te decoderen. Het komt regelmatig voor dat i-Finish verzoeken krijgt van nabestaande die geen toegang hebben tot de iPhone van hun dierbare. Maar ook i-Finish kan de iOS 8.0 en nieuwere versies van de iOS software niet kraken. Nabestaanden nemen dan contact op met Apple. Maar het bedrijf geeft direct aan dat het technisch niet mogelijk is om toegang te verschaffen tot de iPhone. Apple kan de apparatuur wel op “factory settings” zetten. Daarbij worden alle data weggehaald en wordt het apparaat teruggezet naar fabrieksinstellingen.[90] Dan kunnen nabestaanden gebruik maken van de iPhone of laptop. Maar nabestaanden willen dat niet; ze willen juist inzage in de data van hun dierbare. Een overzicht van de mogelijkheden voor nabestaanden om inzage te krijgen in digitale data wordt weergegeven in figuur 11.



Figuur 11. *De mogelijkheden voor een rechtmatige erfgenaam rondom de digitale gegevensdragers van een overledene.*

Nabestaanden kunnen een verzoek sturen aan de OvJ om inzage te krijgen in de digitale gegevens in het dossier. Nabestaanden kunnen zelf ook gegevens inzien die lokaal staan opgeslagen op de laptop of mobiel van de overleden persoon. Maar de sterke beveiliging van Apple belemmert dit proces. Zoals eerder besproken is Apple vaak niet bereid om mee te werken. Erfgenamen kunnen via de rechter proberen om Apple te dwingen om mee te werken. Het is aan de rechter te bepalen of Apple toegang moet gegeven tot de apparatuur.

Hoofdstuk 5: Conclusie

De centrale hoofdvraag van dit onderzoek is als volgt geformuleerd: *Op welke wijze kunnen opsporingsambtenaren en nabestaanden zichzelf op een juridisch correcte wijze toegang verschaffen tot digitale data bij overlijdensgevallen met suïcide als vermoedelijke toedracht?* Om antwoord te kunnen geven op de hoofdvraag is er onderzoek gedaan naar de bestaande wet- en/of regelgeving, zijn er interviews afgenomen en is een reële casus geanalyseerd. Hieruit blijkt dat opsporingsambtenaren toegang kunnen krijgen tot digitale gegevens van overledenen als er sprake is van een verdenking van een art. 67 lid 1 Sv. In dit geval kan een opsporingsambtenaar computers en telefoons in beslag nemen. De opsporingsambtenaar mag zonder tussenkomst van de OvJ onderzoek verrichten aan een in beslag genomen computer en mag daarvoor gebruik maken van technische tools. Een opsporingsambtenaar heeft toestemming nodig van de OvJ om onderzoek te doen aan een in beslag genomen smartphone, als de opsporingsambtenaar meer dan een gering aantal gegevens wil raadplegen.
Een technische tool die data uit een telefoon extraheert kan notificaties van Facebook extraheren. Het raadplegen van een Facebook app is geen deel van het onderzoek aan een in beslag genomen digitale gegevensdrager. Het inloggen in of het raadplegen van de app van Facebook is een vorm van binnendringen in een geautomatiseerd werk. Binnendringen is alleen toegestaan onder strikte voorwaarden. Bovendien kunnen Facebookgegevens opgeslagen staan op een buitenlandse server en daarmee bestaat er de kans dat de soevereiniteit van een ander land geschonden wordt. De infrastructuur van het internet is tegenwoordig zo ingewikkeld dat het veel tijd kan kosten om te achterhalen op welke server deze gegevens staan. De Nederlandse politie kan via een internationaal rechtshulpverzoek Facebookgegevens vorderen als er sprake is van een verdenking van een misdrijf. Omdat het maanden kan duren voordat de aanvraag van een rechtshulpverzoek afgewikkeld wordt, is de drang groot om zelf in te loggen in het Facebook account.

Een verdenking van een misdrijf art. 67 lid 1 Sv kan blijken uit het onderzoek door de forensische arts, of de tactische recherche of de forensische opsporing. Als uit het politieonderzoek blijkt dat er geen aanwijzingen zijn van een misdrijf en de OvJ besluit het onderzoek te sluiten, dan kan er niet meer gesproken worden van een strafvorderlijk belang. Het is onduidelijk of een nabestaande een verzoek kan indienen bij de politie om onderzoek te laten verrichten aan een digitale gegevensdrager van een overledene als uit het vooronderzoek bleek dat er geen aanwijzingen zijn van een strafbaar feit. Dit omdat het niet duidelijk is hoe deze gegevens beschermd worden na de dood. Door de afwezigheid van een strafvorderlijk belang is een opsporingsambtenaar niet bevoegd om in te loggen in het Facebook account van de overledene of om gegevens van Facebook of Apple te vorderen.

De huidige wet- en/of regelgeving zorgt ervoor dat de rechtmatige erfgenaam toegang mag verschaffen tot fysieke, digitale gegevensdragers van de overledene omdat dit zaken zijn en dus overgedragen worden aan de rechtmatige erfgenaam. De algemene voorwaarden van Facebook bepalen dat Facebook accounts niet overdraagbaar zijn. Het gevolg hiervan is dat de rechtmatige erfgenaam niet mag inloggen in het Facebook account van de overledene.

Een Nederlandse rechter heeft (nog) niet bepaald of de algemene voorwaarden van Facebook bezwarend zijn.

Hoofdstuk 6: Aanbevelingen

Aanbeveling 1: onderzoek naar overige elektronicabedrijven en online diensten
Dit onderzoek geeft een beeld van de rechten van opsporingsambtenaren en nabestaanden in het kader van Apple apparatuur en Facebook. Naast Apple zijn nog meer elektronicabedrijven zoals Microsoft en Sony die onderzocht moeten worden. Verder bestaan er veel meer online diensten die ook onderzocht moeten worden. WhatsApp, YouTube, Snapchat, Twitter, Pinterest, LinkedIn en Instagram zijn naast Facebook de meest gebruikte social media platformen in Nederland.[11,12,13] Hiernaast zijn er ook andere online diensten zoals e-mail diensten Gmail, en Outlook en cloud-diensten zoals iCloud, Dropbox en Google Drive. [93] Er moet achterhaald worden hoe en wanneer opsporingsambtenaren toegang kunnen krijgen tot deze digitale data en hoe bereidwillig deze diensten zijn in het delen van deze data. Voor de nabestaanden is het van belang om de algemene voorwaarden van de online diensten te analyseren en te bepalen in hoeverre deze algemene voorwaarden nabestaanden belemmeren om toegang te krijgen. Vervolgens moet onderzocht worden hoe het erfrecht steun kan bieden om toegang te krijgen tot deze data.

Aanbeveling 2: procedure introduceren voor nabestaanden
In de digitale wereld van nu worden er veel digitale sporen achtergelaten op bijvoorbeeld smartphones en computers. Over het algemeen bevat een smartphone meer privacygevoelige gegevens dan een computer, gezien men vaker gebruik maakt van zijn of haar smartphone. Nabestaanden hechten daarom ook veel waarde aan de smartphone van de overledene maar beschikken niet over de tools om toegang te krijgen tot de smartphone. Er moet een procedure geïntroduceerd worden die nabestaanden de mogelijkheid biedt om een verzoek in te dienen bij de politie om onderzoek te laten verrichten aan de smartphone van een overledene bij overlijdensgevallen met suïcide als vermoedelijke toedracht. Er moet een criteria ontwikkeld worden waaraan de politie kan beoordelen of het onderzoek nodig is. Nadat er onderzoek is gedaan aan de smartphone moet de OvJ beoordelen of het delen van de bevindingen ten behoeve van rouw-of traumaverwerking zwaarder weegt dan de privacybelangen van anderen. Indien de smartphone niet beschikbaar is, kan de computer van het slachtoffer onderzocht worden.

Aanbeveling 3: onderzoek naar de samenwerking met Apple en Facebook
Opsporingsambtenaren kunnen via een internationaal rechtshulpverzoek gegevens vorderen. Rechtshulpverzoeken kunnen het proces vertragen, omdat het maanden kan duren voordat het verzoek wordt afgewikkeld. Het is op basis van de transparency rapporten van Facebook en Apple niet te achterhalen hoe vaak de Nederlandse politie samenwerkt met deze bedrijven omdat de transparency rapporten gebaseerd zijn op verzoeken vanuit de Nederlandse overheid. Bovendien is het onbekend of de transparency rapporten gebaseerd zijn op officiële rechtshulpverzoeken of op basis van een goede directe samenwerking.

Samenwerking met Apple is van belang omdat Apple apparatuur steeds beter beveiligd wordt. Hoewel Apple zelf ook geen toegang kan verschaffen tot Apple apparatuur kan Apple kan wel logboeken van de activiteiten van Apple gebruikers verschaffen aan de politie.

Samenwerking met Facebook is van belang omdat de politie zichzelf alleen in uitzonderlijke situaties toegang mag verschaffen tot een Facebook account. Bij overlijdensgevallen met suïcide als vermoedelijk toedracht moet de politie eerst toestemming vragen aan Facebook.

Samenwerking met Facebook en Apple is dus een belangrijk manier voor opsporingsambtenaren om toegang te krijgen tot digitale data. Er moet onderzocht worden hoe de politie samenwerkt met Facebook en Apple en hoe deze samenwerking, indien nodig, optimaler en sneller kan verlopen. Dit kan gedaan worden door interviews af te nemen. Relevante respondenten zijn digitale coördinators van de Nederlandse politie en Officieren van Justitie. De interviews moet aangeven hoe de samenwerking nu verloopt en waar de politie tegen aan loopt.

Aanbeveling 4: het aanpassen van de huidige wetgeving in het kader van het erfrecht
Het probleem van het huidige erfrecht is dat de algemene voorwaarden van een online dienst bepalen wat er met de data van een overleden gebruiker gebeuren. Het erfrecht moet zodanig uitgebreid worden dat er een wettelijke grondslag bestaat op basis waarvan erflaters kunnen bepalen wat er met hun data moeten gebeuren na overlijden, zoals de RUFADAA dat in Amerika biedt. Het resultaat hiervan kan zijn dat de algemene voorwaarden van een online dienst van toepassing zijn, mits de gebruiker tijdens leven toestemming heeft gegeven om zijn of haar digitale data openbaar te maken.
Het overdragen van **de inhoud** van een account is alleen mogelijk als het vermogensrecht zodanig wordt aangepast dat een online account vatbaar is voor overdracht.

Het maken van een nieuwe wet begint bij het schrijven van een wetsvoorstel en een Memorie van Toelichting. Dit wordt gemaakt in opdracht van de betrokken minister.[94] Het ministerie van Justitie en Veiligheid houdt zich onder andere bezig met het privaatrecht. Het vermogensrecht behoort tot het privaatrecht en het erfrecht is onderdeel van het privaatrecht. Een verandering in het vermogensrecht en daarmee een aanpassing in het erfrecht kan gedaan worden in opdracht van de minister van Justitie en Veiligheid, Ferdinand Grapperhaus.

Bronnenlijst

1. Zitvast H. Moeder van verongelukte Dascha [internet] 2018; 24 december. Geraadpleegd op 8 april 2019 via: https://vrouw.nl/artikel/verhalen-achter-het-nieuws/39525/moeder-van-verongelukte-dascha-ik-zing-niet-meer-mee-met?utm_source=google&utm_medium=organic
2. More Than Investigation. Dascha Tamarah Graafsma “Het meisje van de trein” [rapport] 2019; 9 april. Geraadpleegd op 1 juni 2019 via: https://drive.google.com/file/d/1MGVZY-tVD5DhazdMTZ0qdv3vwAIlal7f/view?fbclid=IwAR3cMAbkzs0QaJS36qGmkvgksczmV4ZSCp74GwLnFhWrCdAq_qKmx5fMW08
3. Rurup M, Ufkes D, Limmen R. Hoe spoor je de (bijna) perfecte moord op?. Den haag, Nederland: Politie; 2019
4. McKinnon, L. Planning for the succession of digital assets. Computer Law & Security Review 2011, 4(27): 362-367. https://doi.org/10.1016/j.clsr.2011.03.002
5. Sunde N, Dror I. Cognitive and human factors in digital forensics: Problems, challenges, and the way forward 2019, 29: 101–108. https://doi.org/10.1016/j.diin.2019.03.011
6. Schrikkema, M. De digitale erfenis, hoe regel je dat en wie mag wat bekijken? [internet] 2018; 3 juli. Geraadpleegd op 14 maart 2019, van https://eenvandaag.avrotros.nl/item/de-digitale-erfenis-hoe-regel-je-dat-en-wie-mag-wat-bekijken/
7. Lassche, H. Digitalisering en de opsporingspraktijk Juridische aspecten [pdf] 2019; maart. Geraadpleegd op 8 april 2019, van https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/90036.PD
8. Brouwer, E. Digitale erfenis is veelal een zoektocht [pdf] 2018; 15 oktober. Geraadpleegd op 8 april 2019, van https://i-finish.nl/wp-content/uploads/sites/126/2018/10/Digitale-erfenis-Haarlems-Dagblad-15-10-2018.pdf
9. Digitale Nazorg. Digitale erfenis & online nalatenschap [internet] z.d. Geraadpleegd op 20 februari 2019, van https://digitalenazorg.nl/onze-diensten/
10. Van der Meer I, Sival R, Van der Veer N. Nationale Social Media Onderzoek 2016 [pdf] z.d. Geraadpleegd op 20 februari 2019, van https://www.newcom.nl/uploads/images/Publicaties/Newcom-Nationale-Social-Media-Onderzoek-2016.pdf+
11. Newcom. Social media onderzoek 2017 [internet] 2017; 23 januari. Geraadpleegd op 20 februari 2019, van https://www.newcom.nl/socialmedia2017
12. Peters O, Hoekstra H, Boekee S, Van der Veer N. Nationale Social Media Onderzoek 2018 [pdf] 2018; 29 januari. Geraadpleegd op 20 februari 2019, van https://www.bindinc.nl/wp-content/uploads/2018/04/Newcom-Nationale-Social-Media-Onderzoek-2018-3.pdf
13. Öhman C, Watson D. Are the dead taking over Facebook? A Big Data approach to the future of death online 2019, 6(1): 1-5

14. Apple. Change Passwords preferences in Safari on Mac [internet] z.d. Geraadpleegd op 13 mei 2019, van https://support.apple.com/guide/safari/passwords-sfri40599/mac
15. Scott,B. Who Gets Your Data After Death? Accessing and Managing a Deceased Person's Digital Remnants [internet] 2019; 1 maart. Geraadpleegd op 13 mei 2019, van https://www.iperity.com/tech-culture/data-of-the-dead-what-happens-to-our-data-after-we-die/
16. GrayKey. Magnet Forensics [internet] z.d. Geraadpleegd op 8 mei 2019, van https://www.magnetforensics.com/graykey/
17. Nederlandse Grondwet [Grondwet]. Geraadpleegd op 5 mei 2019, van https://wetten.overheid.nl/BWBR0001840/2018-12-21
18. Van Helden, J. Een kleine geschiedenis van de privacywetgeving [internet] 2018; 10 augustus. Geraadpleegd op 8 mei 2019, van https://www.declercq.com/kennisblog/een-kleine-geschiedenis-van-de-privacywetgeving/
19. European Data Protection Supervisor. The History of the General Data Protection Regulation [internet] z.d. Geraadpleegd op 8 mei 2019, van https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en
20. Wet General Data Protection Regulation artikel 27. Geraadpleegd op 5 mei 2019, van http://www.privacy-regulation.eu/en/article-27-representatives-of-controllers-or-processors-not-established-in-the-union-GDPR.htm
21. Bird & Bird. GDPR Tracker - Personal data of deceased persons. Z.d. Geraadpleegd op 8 mei 2019, van https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/deceased-persons
22. Wetboek van Strafrecht [wetboek]. Geraadpleegd op 8 april 2019, van https://wetten.overheid.nl/BWBR0001854/2019-04-01
23. Burgerlijk Wetboek Boek 7 [wetboek]. Geraadpleegd op, 8 maart 2019, van https://wetten.overheid.nl/BWBR0005290/2019-03-16
24. Hoge Raad. ECLI:NL:PHR:2008:BD7817 [jurisprudentie] 2008; 21 oktober. Geraadpleegd op 8 maart 2019, van https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:PHR:2008:BD7817
25. Wet op de lijkbezorging [wet]. Geraadpleegd op 5 mei 2019, van https://wetten.overheid.nl/BWBR0005009/2018-08-01
26. Auteurswet [wet]. Geraadpleegd op 5 mei 2019, van https://wetten.overheid.nl/BWBR0001886/
27. Autersrecht. Portretrecht [internet] z.d. Geraadpleegd op 20 februari 2019, van https://www.auteursrecht.nl/auteursrecht/Portretrecht
28. Engelfriet, A. De wet op internet. Eerste editie. Amsterdam: Lus Mentis BV ; 2019
29. Facebook. Terms of Service [internet] z.d. Geraadpleegd op 20 februari 2019, van https://www.facebook.com/unsupportedbrowser
30. Mag ik een foto of plaatjes die ik op internet vind gebruiken voor mijn site of blog? [internet] z.d. Geraadpleegd op 20 februari 2019, van https://www.auteursrecht.nl/auteursrechtwijzer/Mag-ik-fotos-of-plaatjes-van-internet-gebruiken
31. Berlee, A. Digital Inheritance in the Netherlands. Journal of European Consumer and Market Law 2017, 6: 1–3

32. Duivestein S, Bloem J. De zwarte kant van sociale media [pdf] 2012. Geraadpleegd op 27 februari 2019, van https://blog.vint.sogeti.com/wp-content/uploads/2013/01/De-Zwarte-Kant-van-Sociale-Media-MF.pdf
33. Chu, N. Protecting Privacy after Death. Northwestern Journal of Technology and Intellectual Property 2015, 13(2): 259–275.
34. Walker, M. (2017). The new uniform digital assets law: estate planning and administration in the information age [pdf] 2017. Geraadpleegd op 4 april 2019, van https://www.americanbar.org/content/dam/aba/publications/real_property_trust_and_estate_law_journal/v52/01/rpte-journal-2017-52-1-article-new-uniform-digital-assets-law-estate-planning-and-administration-in-information-age%20.authcheckdam.pdf
35. Svrnotarissen. Brochure Erfrecht [pdf] z.d. Geraadpleegd op 4 april 2019, van http://www.svrnotarissen.nl/brochure-erfrecht.pdf
36. Burgerlijk Wetboek Boek 4 [wetboek] Geraadpleegd op, 8 maart 2019, van https://wetten.overheid.nl/BWBR0002761/2018-09-19
37. Goed Vertegenwoordigd. Toelichting volmachten [internet] z.d. Geraadpleegd op 30 april 2019, van https://www.goedvertegenwoordigd.nl/maatregelen/volmacht-en-levenstestament/toelichting-volmachten/
38. Koninklijke Notariële Beroepsorganisatie. Een erfenis, wat nu? [pdf] 2010. Geraadpleegd van https://amstelveennotaris.nl/wp-content/uploads/2011/12/KNB-Brochure-Erfrecht-II-Een-erfenis-wat-nu.pdf
39. Korteweg D, Borgesius F. E-Mail na de dood. Juridische bescherming van privacybelangen 2009, 12(5): 213-216
40. Facebook. How do I report a deceased person or an account on Facebook that needs to be memorialized? [internet] z.d. Geraadpleegd op 10 april 2019, van https://www.facebook.com/unsupportedbrowser
41. Apple. Legal Process Guidelines Government & Law Enforcement outside the United States [internet] z.d. Geraadpleegd op 10 april 2019, van https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf
42. Ziccardi, G. Voor eeuwig online. Amsterdam, Nederland: Xander Uitgevers BV; 2018
43. Wetboek van Strafvordering [wetboek]. Geraadpleegd op 8 april 2019, van https://wetten.overheid.nl/BWBR0001903
44. Tweede Kamer der Staten-Generaal. Kamerstuk 34372, nr. 3 Officiële bekendmakingen [Kamerstuk] 2015; 28 december. Geraadpleegd op 8 mei 2019, van https://zoek.officielebekendmakingen.nl/kst-34372-3.html
45. Rechtbank Amsterdam. ECLI:NL:RBAMS:2018:3297 [jurisprudentie] 2018; 16 mei. Geraadpleegd op 8 april 2019, van https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2018:3297
46. Horsman, G. Tool testing and reliability issues in the field of digital forensics 2019; 28 163-165. https://doi.org/10.1016/j.diin.2019.01.009
47. De Gruijter, M. Crime stories (Scriptie) 2012; maart. Geraadpleegd van https://www.njb.nl/Uploads/2014/1/Masterscriptie-Gruijter.pdf
48. Lettinga, B. Een onderzoek naar de theorie en praktijk van hypothese en scenariovorming in de opsporing [internet] 2009. Geraadpleegd van https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/74802.pdf

49. Artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden [wetsartikel]. Geraadpleegd op 8 april 2019, van https://wetten.overheid.nl/BWBV0001000/2010-06-10
50. Mevis P, Verbaan J, Salverda B. Onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken ten behoeve van de opsporing en vervolging van strafbare feiten [pdf] 2016. Geraadpleegd op 6 juni 2019, van https://www.wodc.nl/binaries/2598-volledige-tekst_tcm28-74084.pdf
51. Rechtbank Amsterdam. ECLI:NL:RBAMS:2015:2183 [jurisprudentie] 2015; 19 maart. Geraadpleegd op 8 april 2019, van https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2015:2183
52. Hoge Raad.,ECLI:NL:HR:2017:584 [jurisprudentie] 2017; 4 april. Geraadpleegd op 8 april 2019, van https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2017:584
53. Gerechtshof Amsterdam. ECLI:NL:GHAMS:2018:1435 [jurisprudentie] 2018; 23 april. Geraadpleegd op 8 april 2019, van https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHAMS:2018:1435
54. Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv [aanwijzing wet]. Geraadpleegd op 20 mei 2019, https://wetten.overheid.nl/BWBR0041956/2019-03-01
55. Nederlands Juristenblad. Europees onderzoeksbevel [internet] 2017; 21 juni. Geraadpleegd op 16 mei 2019, van https://www.njb.nl/wetgeving/staatsbladen/europees-onderzoeksbevel.21026.lynk
56. Facebook. Information for Law Enforcement Authorities [internet] z.d. Geraadpleegd op 1 mei 2019, van https://www.facebook.com/unsupportedbrowser
57. Facebook. Law Enforcement Guidelines [pdf] 2010. Geraadpleegd op 1 mei 2019, van https://www.eff.org/files/filenode/social_network/facebook2010_sn_leg-doj.pdf
58. Wet politiegegevens [wet]. Geraadpleegd op 24 april 2019, van https://wetten.overheid.nl/BWBR0022463/2019-05-01
59. Aanwijzing Wet justitiële en strafvorderlijke gegevens [aanwijzing wet]. Geraadpleegd op 24 april 2019, van https://wetten.overheid.nl/BWBR0041090/2018-07-01
60. Wet op de rechterlijke organisatie [wet]. Geraadpleegd op 24 april 2019, van https://wetten.overheid.nl/BWBR0001830/2019-01-01
61. Ferdie Migchelbrink Consultancy. Half open en volledig gestructureerde of gestandaardiseerde interviews [internet] z.d. Geraadpleegd op 5 mei 2019, van http://www.actie-onderzoek.nl/pdf/gestructureerde%20interviewswebsitegereed.pdf
62. Taskforce lijkschouw en gerechtelijke sectie. De dood als startpunt [pdf] 2018. Geraadpleegd op 9 juni 2019, van Taskforce lijkschouw en gerechtelijke sectie De dood ... - Rijksoverheidhttps://www.rijksoverheid.nl/...taskforce-lijkschouw-en-gerechtelijke-sectie/tk-bijlage-t...
63. Nederlandse Vereniging voor Kindergeneeskunde. NODOK [internet] z.d. Geraadpleegd op 8 mei 2019, van https://www.nvk.nl/Nieuws/Dossiers/NODO
64. Nederlandse Vereniging voor Kindergeneeskunde. Handelingsprotocol “Nader Onderzoek naar de DoodsOorzaak bij Kinderen” [pdf] 2016; 16 juli. Geraadpleegd op 8 mei 2019, van

https://www.nvk.nl/DeNVK/Documenten.aspx?Command=Core_Download&EntryId=14045
65. Jansen, B. Inzake Opsporing on-line, het volledige rapport van de enquêtecommissie opsporingsmethoden en het Rijksrechercherapport RCID Kennemerland [internet] 1999. Geraadpleegd op 9 juni 2019 van https://www.burojansen.nl/traa/index.htm
66. Aanwijzingen inbeslagneming [aanwijzing wet]. Geraadpleegd op 8 mei 2019, van https://wetten.overheid.nl/BWBR0029019/2014-07-01
67. Cellebrite. Extract & decode [internet] z.d. Geraadpleegd op 15 mei 2019, van https://www.cellebrite.com/en/product/solutions/extract-decode/
68. Grapperhaus, F. Wettelijke mogelijkheden standaard bloedonderzoek bij verkeersongevallen - Forensische zorg. KST3362843 [Kamerstuk] 2019; 14 maart. Geraadpleegd op 21 mei 2019, van https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vkwtm95zheyi
69. B.C. van Beers. Commentaar op artikel 11 van de Grondwet [pdf] 2013. Geraadpleegd op 9 juni 2019, van DE GRONDWET - ARTIKEL 11 ... - Nederland rechtsstaathttps://www.nederlandrechtsstaat.nl/module/nlrs/.../printPdf_v2.asp...
70. Rechtbank Amsterdam. ECLI:NL:RBROT:2019:2712 [jurisprudentie] 2019; 22 februari. Geraadpleegd op 15 mei 2019, van https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBROT:2019:2712
71. Facebook. Basic Privacy Settings & Tools [internet] z.d. Geraadpleegd op 23 april 2019, van https://www.facebook.com/unsupportedbrowser
72. Taylor M, Haggerty J, Gresty D, Almond P, Berry T. Forensic investigation of social networking application 2014, 2014(11), 9–16. https://doi.org/10.1016/s1353-4858(14)70112-6
73. Kop N, Wal R, Snel G. Over strategieën in de opsporingspraktijk [pdf] 2011. Geraadpleegd op 9 juni 2019, van https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/82557.pdf
74. Rechtbank Noord Holland. ECLI:NL:RBNHO:2019:1568 [jurisprudentie] 2019; 28 februari Geraadpleegd op 9 juni 2019 van, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBNHO:2019:1568
75. Apple. Government Information Requests Netherlands [internet] z.d. Geraadpleegd op 23 mei 2019, van https://www.apple.com/legal/transparency/nl.html
76. Facebook. Request For User Data [internet] z.d. Geraadpleegd op 23 mei 2019, van https://transparency.facebook.com/government-data-requests/country/NL
77. Openbaar Ministerie. Klacht niet vervolging (art.12 Sv) [internet]. Z.d. Geraadpleegd op 23 mei 2019, van https://www.om.nl/contact/klachten/klacht-vervolging/
78. TjongTjin Tai, E. Data in het vermogensrecht. WPNR: Weekblad voor privaatrecht, notariaat en registratie 2015, 149(7085): 993-998.
79. Engelfriet, A. Computervredebreuk: wanneer is dit het geval? [internet] z.d. Geraadpleegd op 9 april 2019, van https://ictrecht.nl/juridisch-advies/computervredebreuk/
80. Rechtbank Den Haag. ECLI:NL:RBDHA:2018:10451 [jurisprudentie] 2018; augustus 30. Geraadpleegd op 15 mei 2019, van https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2018:10451

81. Rechtbank Overijssel. ECLI:NL:RBOVE:2019:160 [jurisprudentie] 2019; januari 22. Geraadpleegd op 15 mei 2019, van https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOVE:2019:160
82. Rechtbank Oost-Brabant. ECLI:NL:RBOBR:2013:BZ1157 [jurisprudentie] 2013; 15 mei. Geraadpleegd op 15 mei 2019, van https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOBR:2013:BZ1157
83. Koninklijke Notariële Beroepsorganisatie. Over KNB [internet] z.d. Geraadpleegd op 10 mei 2019, van https://www.knb.nl/over-knb
84. Van Mourik M, Schols F. Erfrecht. Deventer, Nederland: Wolters Kluwer; 2018.
85. Ensie. Codicil [internet] 2016; 16 februari. Geraadpleegd op 11 april 2019, van https://www.ensie.nl/familiezaken/codicil
86. Art. 1 van het Burgerlijk Wetboek 3 [wetsartikel]. Geraadpleegd op 16 april 2019, van https://wetten.overheid.nl/BWBR0005291/2019-01-01
87. Art. 2 van het Burgerlijk Wetboek 3 [wetsartikel]. Geraadpleegd op 16 april 2019, van https://wetten.overheid.nl/BWBR0002656/
88. Lisicka, A. Are parents entitled to access the Facebook account of a deceased child? [internet] 2018; 9 april. Geraadpleegd op 25 april 2019, van https://newtech.law/en/are-parents-entitled-access-the-facebook-account-of-a-deceased-child/
89. Deutsche Welle. German court says parents can inherit Facebook data [internet] 2018; 12 juli. Geraadpleegd op 25 april 2019, van https://www.dw.com/en/facebook-court-rules-parents-have-rights-to-dead-daughters-account/a-44642230
90. Brubaker J,Callison V. (2016). Legacy Contact. Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems 2016; 16: 2-8. https://doi.org/10.1145/2858036.2858254
91. Apple. macOS Security [internet] 2018; maart. Geraadpleegd op 25 april 2019, van https://www.apple.com/business/resources/docs/macOS_Security_Overview.pdf
92. Apple. Use FileVault to encrypt the startup disk on your Mac [internet] 2018; 30 november. Geraadpleegd op 8 mei 2019, van https://support.apple.com/en-us/HT204837
93. Smith, S. Gratis e-mailprogramma's [internet] 2019; 23 januari. Geraadpleegd op 9 juni 2019, van https://www.consumentenbond.nl/alles-in-1/beste-e-mailprogramma
94. Rijksoverheid. Hoe komt een wet tot stand [internet] z.d. Geraadpleegd op 9 juni 2019, van https://www.rijksoverheid.nl/onderwerpen/wetgeving/hoe-komt-een-wet-tot-stand

Bijlagen

Bijlage 1. *Staten van de Europese Unie die regels hebben omtrent het verwerken van persoonsgegevens van overledenen.*

Staat	*Regelgeving omtrent verwerking van gegevens van overledenen*
Denemarken	De AVG is van toepassing op data van overledenen voor een periode van tien jaar.
Frankrijk	Tijdens leven kunnen personen vastleggen wat hun wens is omtrent de verwerking van hun persoonsgegevens.
Italië	In het geval dat een erfgenaam of familielid de privacy van de overledene wil beschermen, kunnen sectie 15 tot en met 22 van de GDPR van geactiveerd worden.
Spanje	Erfgenamen hebben het recht om toegang te krijgen tot gegevens van de overledene en het recht om een verzoek te doen tot verwijdering van deze gegevens. Dit is niet van toepassing indien de overledene tijdens leven heeft aangegeven dat hij dit niet wil. Verder wordt in de wet aangegeven hoe online diensten toegang moeten geven tot gegevens van overledenen.
Hongarije	Er is een wetsvoorstel opgesteld waarin staat beschreven hoe een erfgenaam of vertrouwenspersoon het recht heeft om een verzoek te maken voor het verwijderen van gegevens of beperken van het verwerken van deze gegevens binnen een periode van vijf jaar na overlijden.
Slowakije	Gegevens van overledenen mogen verwerkt worden wanneer de naaste personen er toestemming voor geven.