KONINKLIJKE NEDERLANDSE
AKADEMIE VAN WETENSCHAPPEN

ETHISCHE EN JURIDISCHE ASPECTEN VAN INFORMATICAONDERZOEK

ADVIES

ETHISCHE EN JURIDISCHE ASPECTEN VAN INFORMATICAONDERZOEK

Koninklijke Nederlandse Akademie van Wetenschappen
Postbus 19121, 1000 GC Amsterdam
Telefoon + 31 20 551 0700
knaw@knaw.nl
www.knaw.nl

pdf beschikbaar op www.knaw.nl

Basisvormgeving: Edenspiekermann, Amsterdam
Engelse vertaling samenvatting: Balance, Maastricht
Opmaak, bureauredactie en index: Ellen Bouma, Alkmaar

Illustratie omslag: Istock, the light-writer

ISBN 978-90-6984-709-2

Het papier van deze uitgave voldoet aan ∞ iso-norm 9706 (1994) voor permanent houdbaar papier.

Deze publicatie kan als volgt worden aangehaald: KNAW (2016). *Ethische en juridische aspecten van informaticaonderzoek*, Amsterdam, KNAW.

ETHISCHE EN JURIDISCHE ASPECTEN VAN INFORMATICA-ONDERZOEK

Koninklijke Nederlandse Akademie van Wetenschappen
September 2016

VOORWOORD

Wetenschap is fascinerend en de resultaten ervan zijn vaak van grote invloed op de maatschappij. Dat geldt voor veel wetenschapsgebieden maar het geldt zeer zeker voor de informatica. De ontwikkelingen in dit vakgebied zorgen ervoor dat we op totaal andere manieren met elkaar communiceren dan tien jaar geleden. Informatici maken het mogelijk om auto's zonder bestuurder te laten rijden en zorgen dat we wereldwijd veilig met onze bankpas kunnen betalen. Juist vanwege deze enorme invloed is het van belang dat we ons ook rekenschap geven van de mogelijke negatieve effecten van informaticaonderzoek. Mag alles wat kan? Mag je bijvoorbeeld voor onderzoek naar de veiligheid van computersystemen inbreken in het systeem van een bank? Hoe borg je de privacy van deelnemers aan wetenschappelijk onderzoek? Wetenschappers moeten zich steeds vaker buigen over dit soort ethische en juridische vraagstukken. Dat is niet altijd eenvoudig en veel onderzoeksgebieden ontberen nog een kader voor de ethische beoordeling. Ik ben dan ook bijzonder verheugd dat de informaticaonderzoekers uit onze Adviesraad voor de Technische Wetenschappen, Wiskunde, Informatica, Natuur- en Sterrenkunde en Scheikunde (TWINS Raad) het initiatief hebben genomen voor dit adviesrapport.

De commissie, onder voorzitterschap van Jan Willem Klop, heeft grondig in kaart gebracht hoe ethische en juridische dilemma's door onderzoekers kunnen worden beoordeeld. Ze heeft daarbij goed gekeken naar de medische wetenschappen, waar dit soort toetsingskaders al veel langer bestaat, en haar licht opgestoken bij buitenlandse collega's.

De commissie beveelt onder meer aan om ethische beoordelingscommissies in te stellen en laat haar licht schijnen over de werkwijze van die commissies. Ik ondersteun

dit pleidooi van harte, maar teken daarbij aan dat we moeten voorkomen dat alle universitaire beoordelingscommissies hun eigen lokale toetsingskader gaan ontwikkelen. Het is immers moeilijk uit te leggen dat onderzoek dat in Groningen wordt goedgekeurd, in Nijmegen op ethische gronden ontoelaatbaar wordt geacht. Ik hecht daarom sterk aan het lerende model dat door de commissie wordt voorgesteld. Van groot belang daarbij is het toegankelijk maken van de beoordelingen van de commissies op een centrale plaats. Ik roep de informaticaonderzoekers op om hier snel werk van te maken.

Mij spreekt bijzonder aan dat de commissie benadrukt dat het instellen van beoordelingscommissies de individuele onderzoekers niet van eigen verantwoordelijkheid ontslaat. Hier ligt een belangrijke taak voor het wetenschappelijk onderwijs: toekomstige generaties onderzoekers hiervan bewust te maken. Sommige onderzoeksscholen hebben ethiek al een onderdeel gemaakt van het verplichte curriculum voor hun jonge onderzoekers in opleiding. Ik hoop dat andere onderzoeksscholen dit voorbeeld spoedig zullen volgen.

Dit adviesrapport richt zich tot de informaticagemeenschap. Maar ook andere wetenschapsgebieden stuiten op ethische dilemma's die ogenschijnlijk inherent zijn aan het informaticaonderzoek. Bovendien raakt informatica steeds meer verweven met andere gebieden. Ik hoop en verwacht daarom dat dit adviesrapport voor andere disciplines een inspiratiebron zal blijken.

Ten slotte nog een opmerking over de scope van het advies. Bij de start van dit adviestraject had de commissie ook de ethische en juridische aspecten van big data in het vizier. Al snel bleek dat dit terrein bijzonder omvangrijk is en zich bovendien uitstrekt ver voorbij de informatica. Daarom heeft de KNAW besloten een aparte commissie big data in te stellen. Het rapport van die commissie kunt u begin volgend jaar verwachten.

José van Dijck
President KNAW

SAMENVATTING

Informaticaonderzoek en de resultaten ervan hebben grote invloed op de samenleving. Het is daarom vanzelfsprekend dat zowel de maatschappij als onderzoeksfinanciers steeds meer een gedegen afweging verwachten over de ethische en juridische dilemma's die aan dit onderzoek zijn verbonden. Mag je bijvoorbeeld een OV-chipkaart of een toegangspas voor alle gebouwen van de rijksoverheid kraken bij een onderzoek naar de veiligheid van dit soort systemen, en zo ja onder welke voorwaarden? Momenteel wordt deze afweging meestal al dan niet expliciet door de betreffende onderzoekers gemaakt. Bij een aantal instellingen wordt echter ook al geëxperimenteerd met ethische commissies. Deze ontwikkeling staat echter nog in de kinderschoenen. De komende jaren moet er een transparant beoordelingskader en een efficiënte infrastructuur voor de beoordeling van de ethische en juridische aspecten van informaticaonderzoek worden ontwikkeld. Met dit advies wil de KNAW een bijdrage leveren aan de verdere professionalisering van het informaticaonderzoeksgebied.

De KNAW heeft hiertoe een commissie ingesteld met de opdracht:
Geef aan hoe informaticaonderzoek beoordeeld kan worden op ethische en juridische aspecten.

De commissie heeft zich vooral gericht op de dilemma's die spelen bij onderzoek zoals dat wordt uitgevoerd aan de Nederlandse informatica-afdelingen en onderzoeksinstituten. Typische voorbeelden hiervan zijn onderzoek naar de beveiliging van netwerken en computersystemen, mens-machine-interactie, betrouwbaarheid van software en kunstmatige intelligentie. De ethische en juridische aspecten die te maken hebben met het verzamelen en gebruiken van grote (privacygevoelige) gegevensverzamelingen vallen buiten de scope van dit advies. Hiervoor heeft de KNAW een afzonderlijke adviescommissie big data ingesteld.

SUMMARY

Informatics research and its results have a huge influence on society. It goes without saying that both the public and research funding bodies increasingly expect an exhaustive review of the ethical and legal dilemmas associated with this research. For example, is it permissible to hack a public transport smartcard or a keycard allowing access to all government buildings when investigating the security of such systems? And if so, subject to which conditions? At the moment, it is up to the researchers themselves to make the ethical and legal judgement call, explicitly or not. And although a number of institutions are experimenting with ethical review boards, such initiatives are still in their infancy. In the years ahead, we must develop a transparent review mechanism and an efficient infrastructure for assessing the ethical and legal aspects of informatics research. The Academy believes that this advisory report will support continuing professional development in the field of informatics research.

The Academy has installed a committee whose task is:
to identify ways to assess the ethical and legal aspects of informatics research.

The committee focused mainly on the dilemmas involved in research such as that conducted by informatics departments at Dutch universities and research institutes. Typical examples include research on network and computer system security, human-machine interaction, software reliability, and artificial intelligence. The ethical and legal aspects associated with collecting and using large (privacy-sensitive) datasets fall outside the scope of this report. The Academy has established a separate 'Big Data' advisory committee to address that subject.

De commissie heeft op verschillende manieren informatie verzameld en geanalyseerd. Allereerst heeft de commissie interviews gehouden met sleutelfiguren in het veld. Op deze manier ontstond een beeld van de manier waarop binnen instellingen tegen dit onderwerp wordt aangekeken, of en zo ja hoe het onderzoek wordt beoordeeld en welke dilemma's men ervaart. Voor het opstellen van een beoordelingskader heeft de commissie protocollen van Nederlandse en buitenlandse instellingen geanalyseerd. In de medische wereld is al veel ervaring opgedaan met ethische beoordeling van onderzoeksvoorstellen. Daarom is gedetailleerd gekeken hoe dit daar is georganiseerd en wat we ervan kunnen leren. Tijdens een klankbordbijeenkomst zijn de hoofdlijnen van het advies gepresenteerd aan het wetenschappelijke veld. De commentaren uit deze bijeenkomst zijn verwerkt in dit eindrapport.

CONCLUSIE 2.1

In de maatschappij in brede zin, maar ook in het bijzonder door onderzoeksfinanciers, wordt meer en meer een gedegen ethische afweging van wetenschappers gevraagd. Dit geldt voor veel vakgebieden maar zeker voor de informatica gezien de enorme maatschappelijk effecten en het belang van dit vakgebied. Het is gewenst dat er binnen dit vakgebied een morele infrastructuur wordt ontwikkeld. Dit betekent dat er een transparant en herkenbaar beoordelingskader moet groeien waarover binnen het vakgebied consensus bestaat. Bovendien moet worden gezocht naar een manier van beoordelen die zorgvuldig en gedegen, maar tegelijkertijd ook efficiënt is en zonder al te veel bureaucratie kan werken.

CONCLUSIE 2.2

In de medische wetenschappen is al veel ervaring opgedaan met ethische beoordeling van onderzoek. Door de sterke focus op de gevolgen voor proefpersonen is die ervaring niet één op één te gebruiken in het geval van informaticaonderzoek. Aan informaticaonderzoek kleven ethische vraagstukken met een geheel eigen karakter. Bovendien ontbreekt bij informaticaonderzoek een wettelijke verplichting op ethische toetsing. Het vakgebied zal daarom met gebruik van de ervaringen uit de medische disciplines zelf een eigen toetsingskader en manier van toetsing moeten ontwikkelen.

In informaticaonderzoek is met grote regelmaat sprake van het verzamelen of bewerken van persoonsgegevens, alsmede van onderzoek gedaan naar software of computersystemen waarvan de eigendomsrechten bij anderen liggen. Hierdoor horen bij dit type onderzoek al snel juridische vragen met betrekking tot bijvoorbeeld privacy of intellectuele eigendomsrechten. Het valt buiten de mogelijkheden van de commissie om volledig in kaart te brengen wat juridisch gezien wel of niet toegestaan is en onder welke voorwaarden en omstandigheden dat het geval is. De commissie schetst daarom voor verschillende fases van een onderzoek veelvoorkomende dilemma's en mogelijke maatregelen om daarmee om te gaan. In specifieke gevallen is het altijd noodzakelijk

The committee collected and analysed information in various ways. First of all, it interviewed key figures in the field. This has allowed it to form a picture of how institutions view this subject, and whether – and if so, how – they review their research and which dilemmas they encounter along the way. As background for developing a review mechanism, the committee analysed the protocols utilised by Dutch and foreign institutions. Medical science has already gained considerable experience in reviewing the ethics of research proposals. The committee therefore looked in detail at how the medical world is organised in that regard and what lessons we can learn from it. The committee presented the main outlines of its report to the research community during a liaison group meeting. The participants' comments at that meeting have been incorporated into this final report.

CONCLUSION 2.1

Society in general, but also – and in particular – research funding bodies are increasingly asking scientists to conduct an exhaustive review of the ethical aspects of their research. That is the case in many disciplines, but certainly in informatics, given its enormous societal impact and importance. We must develop an ethical infrastructure for informatics. This means that a transparent and distinguishable review mechanism must evolve about which the field has reached consensus. In addition, we must seek out an assessment method that is scrupulous and robust but also efficient and functional without being too bureaucratic.

CONCLUSION 2.2

The medical sciences have already gained considerable experience in the ethical scrutiny of research. Because it places heavy emphasis on the consequences for human test subjects, however, the system used in medical research cannot simply be transferred across the board to informatics research. The ethical issues involved in informatics research are highly specific to the field. Moreover, the law does not prescribe any form of ethical assessment for informatics research. That is why informatics can draw on the experiences of the medical disciplines but must develop its own review mechanism and assessment method.

The collection and processing of personal data is very common in informatics research, as are investigations into software or computer systems that are the property of others. That is why this type of research soon raises legal questions, for example concerning privacy or intellectual property rights. It is beyond the committee's remit to conduct an exhaustive study of what the law does and does not permit and the conditions and circumstances that apply in either case. The committee has therefore outlined recurring dilemmas in various phases of research and described potential measures for dealing with them. In specific cases, however, a legal expert should always be consulted. In every phase of research, researchers must be aware of the potential legal implications of their actions. How will my research affect the privacy of

om juridische expertise in te roepen. Het is belangrijk dat onderzoekers zich in alle fases van het onderzoek bewust zijn van de mogelijke juridische implicaties van hun handelen. Wat zijn de gevolgen van mijn onderzoek voor de privacy van anderen? Zijn de handelingen die ik in het kader van mijn onderzoek verricht in overeenstemming met wettelijke regelingen en contractuele afspraken op het terrein van het intellectuele eigendomsrecht? Zorgvuldigheid en goed documenteren is geboden. Minder bekend bij onderzoekers is dat 'niets doen' ook tot aansprakelijkheid kan leiden. Onderzoekers hebben een zorgplicht hetgeen kan betekenen dat ze ongebruikelijke patronen niet zonder risico op juridische sancties kunnen negeren.

CONCLUSIE 3.1

Bij de keuze van een onderzoeksonderwerp moet het wetenschappelijke belang voorop staan en het maatschappelijke belang goed onderbouwd worden. Daarbij moet duidelijk worden gemaakt op welke wijze en in welke mate de bevindingen van het onderzoek eventuele belangen van derden kunnen raken, waaronder de privacy en intellectuele eigendomsrechten. Onderzoekers en andere betrokkenen zullen een expliciete afweging moeten maken tussen het wetenschappelijke belang en maatschappelijke belang van het onderzoek enerzijds en het belang van eventuele derden wier rechten en belangen mogelijk worden geschonden anderzijds. Het doel heiligt kortom niet altijd de middelen.

CONCLUSIE 3.2

Informaticaonderzoekers hebben een zorgplicht. Dit betekent dat passiviteit in bepaalde situaties kan leiden tot aansprakelijkheid. Onderzoekers en onderzoeksgroepen moeten daarom alert zijn en waargenomen risico's voor personen en de samenleving melden binnen de eigen organisatie en waar aan de orde aan handhavende instanties.

Wereldwijd wordt er sinds de jaren tachtig van de vorige eeuw in de ethiek veel aandacht besteed aan de ethische vraagstukken rond ICT. De literatuur hierover is echter overwegend geïnitieerd vanuit de sociale en gedragswetenschappen en heeft vooral betrekking op sociale media en internet. Er bestaat internationaal geen uitgekristalliseerd kader voor beoordelingscommissies op het gebied van informaticaonderzoek. Ook is er nog geen beproefd model voor de manier waarop dit efficiënt georganiseerd kan worden. Zowel voor de maatschappij als voor het onderzoeksveld zelf is het van belang dat dit de komende jaren wordt ontwikkeld. De commissie pleit daarom voor het instellen van lokale *Ethical Review Boards Informatics* (ERBI's). Deze ERBI's hebben in de ogen van de commissie drie belangrijke functies.

1. Het beoordelen van informaticaonderzoek op ethische aspecten. Onderzoeksvoorstellen met duidelijke ethische aspecten gaan dan ook bij voorkeur pas van start na positief advies van de ERBI.
2. Deskundigheidsbevordering, zodat onderzoekers en instellingen, op basis van

others? Do the activities that I am undertaking within the context of my research comply with statutory rules and contractual agreements governing intellectual property rights? Scrupulousness and proper documentation are advised. What many researchers do not realise is that 'doing nothing' can also lead to liability issues. Researchers have a duty of care, which may mean that they run the risk of legal sanctions if they ignore unusual patterns.

CONCLUSION 3.1

When selecting a research subject, researchers should give top priority to the interests of science and offer solid arguments for why their research will serve the interests of society. They should clarify how and to what extent their findings could affect the interests of third parties, including their privacy and intellectual property rights. Researchers and other relevant stakeholders should explicitly weigh the scientific and societal interests of their research against the interests of any third parties whose rights may be infringed. In short, the end does not always justify the means.

CONCLUSION 3.2

Informatics researchers have a duty of care. This means that remaining passive in certain situations could lead to their being held liable. Researchers and research groups should therefore remain vigilant and report any perceived risks to persons and society to compliance officers within their own organisations and, where necessary, to the enforcement authorities.

The ethical issues associated with IT have been the subject of worldwide interest in the field of ethics since the 1980s. The literature addressing this subject, however, can largely be found in the social and behavioural sciences and mainly concerns social media and the internet. There is no well-defined set of international guidelines for review boards in informatics research, nor is there a tried-and-tested model for organising reviews efficiently. Both for society and the research field itself, it is important to develop such a model in the years ahead. The committee therefore favours the installation of local Ethical Review Boards for Informatics (ERBIs). In the committee's view, the ERBIs would have three important tasks:

1. to assess the ethical aspects of informatics research, so that research that clearly raises ethical questions would ideally commence only after the relevant research proposal was given the greenlight by the ERBI.
2. to promote continuing professional development, so that researchers and institutions can account for their informatics research in ethical terms, based on informed judgement;
3. to embody the core and promote the continuity of a community of expertise in which knowledge concerning this subject is documented and continues to advance. The ERBI would thus serve as the linchpin of an organisation's ethical learning process.

weloverwogen oordeelsvorming, ethisch gemotiveerde verantwoording kunnen afleggen over hun informaticaonderzoek.
3. Kern en continuïteit belichamen van een gemeenschap van expertise waarin kennis rond dit onderwerp wordt gedocumenteerd en al doende verder wordt ontwikkeld. De ERBI als spil in het morele leerproces van de organisatie.

De commissie ziet een aantal succesfactoren voor het goed functioneren van deze ERBI's, waaronder de lokale verbondenheid, de snelheid van handelen en de status en legitimiteit van de adviezen. De lokale verbondenheid is van groot belang omdat een ERBI alleen kan functioneren als de afstand tussen deze commissie en onderzoekers zowel fysiek als gevoelsmatig gering is. De commissie pleit daarom voor lokale *review boards*. Het is echter van groot belang dat deze *review board*s onderling een gezamenlijk denkkader (beoordelingskader/handelingskader) ontwikkelen. Een landelijk intervisiemodel kan hierbij helpen.

CONCLUSIE 4.1

Het instellen van een *Ethical Review Board Informatics* en het monitoren van haar prestaties en de reflectie op de aldus verworven inzichten, is een van de manieren waarop de informaticaonderzoeksgemeenschap gestalte kan geven aan haar morele en maatschappelijke verantwoordelijkheid alsmede uitdrukking kan geven aan het besef dat informatica een belangrijke vormgever is van de samenleving.

AANBEVELING 4.1

De commissie raadt alle besturen van instituten of afdelingen actief op het terrein van informaticaonderzoek aan om, al dan niet samen met collega-instellingen, een *Ethical Review Board Informatics* (ERBI) in te stellen. Deze ERBI's hebben als primaire taak het beoordelen van informaticaonderzoek op ethische aspecten. Daarnaast kan een ERBI fungeren als de kern van een gemeenschap waarin kennis rond dit onderwerp verder kan worden ontwikkeld.

AANBEVELING 4.2

De ethische toetsing van informaticaonderzoek staat nog in de kinderschoenen. Er is dan ook geen blauwdruk of ideaalbeschrijving voor een *Ethical Review Board Informatics* te geven en er bestaat ook geen vastgesteld normenkader. Bovendien is informatica een bijzonder dynamisch vakgebied waardoor de informaticavraagstukken van volgend jaar nu nog niet te voorzien zijn. De ERBI's wordt aangeraden voor zichzelf een werkwijze en een normenkader te ontwikkelen en dat te doen in nauw overleg met andere ERBI's.

Het is niet eenvoudig om eenduidig aan te geven welk onderzoek ethische of juridische dilemma's met zich meebrengt en welke risico's dat met zich meebrengt. Toch is het voor de voortgang van het wetenschappelijke onderzoek en voor de efficiënte werking van een ERBI noodzakelijk om zo snel mogelijk de voorstellen te identificeren die

The committee has identified a number of key success factors that will ensure the robustness of these ERBIs, including local engagement, speed of action, and the status and legitimacy of their opinions. Local engagement is hugely important because an ERBI can only function if the distance between the board and the researchers is minimal, both physically and in terms of sentiment. The committee therefore supports the installation of local review boards. It is very important, however, for the boards to develop a shared conceptual framework (review/action mechanisms). A national peer-review model can assist them in this.

CONCLUSION 4.1

One way that the informatics research community can live up to its ethical and public responsibility and demonstrate its awareness that informatics plays an important role in shaping society is to install an Ethical Review Board for Informatics, monitor the performance of this board, and reflect on the lessons learned in this manner.

RECOMMENDATION 4.1

The committee advises all governing bodies of institutes or departments active in informatics research to install an Ethical Review Board for Informatics (ERBI), either on their own or in cooperation with sister institutions. The primary task of the ERBIs is to assess the ethical aspects of informatics research. They can also function as the core of a community in which knowledge concerning this subject continues to advance.

RECOMMENDATION 4.2

Ethical assessment of informatics research is still in its infancy. No blueprint or ideal description of an Ethical Review Board for Informatics can be provided, nor does any set of predetermined standards exist. In addition, informatics is an exceptionally dynamic field, making it impossible to predict which issues will arise next year. ERBIs are advised to develop their own methods and set of standards, and to do so in close consultation with other ERBIs.

It is difficult to pinpoint precisely which type of research will raise ethical or legal dilemmas and the attendant risks. Nevertheless, in the interests of scientific progress and efficiency, an ERBI must identify, as quickly as possible, proposals whose ethical or legal aspects require further examination. As a starting point for discussion within ERBIs, the committee therefore proposes a review procedure that distinguishes between a more lenient and a more stringent assessment. The lenient, and therefore faster, procedure is for research of a more standard nature. The more stringent procedure is for non-standard research. A critical factor in the entire review cycle is the report issued by the ERBI and how it documents and shares the cases it has reviewed. It should preferably do so in a way that allows researchers and all other ERBIs to consult the reports easily. Specifically, that will allow all ERBIs to work together on developing a uniform review mechanism.

ethisch of juridisch gezien nadere beschouwing vergen. Als startpunt voor de discussies binnen de ERBI's doet de commissie daarom een voorstel voor een beoordelingsprocedure waarin een lichte en een zwaardere procedure worden onderscheiden. De lichte en daarmee snellere procedure is voor onderzoek met een meer standaard karakter. De zwaardere procedure is voor niet-standaard onderzoek. Cruciaal in de hele beoordelingscyclus is de rapportage over de advisering en het vastleggen en onderling delen van de behandelde cases. Dit moet bij voorkeur gebeuren op zodanige manier dat de adviezen door onderzoekers en door alle ERBI's eenvoudig te raadplegen zijn. Dit draagt namelijk bij aan het proces om met alle ERBI's gezamenlijk een eensluidend beoordelingskader te ontwikkelen.

CONCLUSIE 5.1

Ethici gebruiken morele waardetypen om de overwegingen bij ethische afwegingsprocessen te articuleren. Voorbeelden van dergelijke waardetypen zijn 'respect', 'privacy' en 'welzijn'. Er zijn echter zeer veel verschillende en uiteenlopende waarden die niet tot elkaar gereduceerd kunnen worden. Waarden kunnen ook niet eenduidig geordend worden en kunnen zelfs onderling conflicterend zijn. Dit geldt ook voor de waarden die veel voorkomen bij informaticaonderzoek. Dit zogenoemde waardenpluralisme maakt dat er geen eenduidig en vastomlijnd beoordelingskader te geven is. Van geval tot geval zal een afweging gemaakt moeten worden.

CONCLUSIE 5.2

De protocollen en richtlijnen die momenteel door veel binnen- en buitenlandse organisaties worden gebruikt bij de ethische beoordeling zijn tamelijk beperkt in scope. De vragen hebben vooral betrekking op de ethische aspecten van identificeerbare onderzoekssubjecten. Ethische aspecten van de effecten van het onderzoek op de maatschappij of milieu worden zelden meegenomen.

AANBEVELING 5.1

ERBI's wordt aangeraden om een efficiënte en transparante procedure te ontwikkelen waarbij onderscheid wordt gemaakt in een lichte en een zwaardere procedure. De lichte procedure is bedoeld voor onderzoeksvoorstellen die meer standaardonderzoek betreffen. In dit adviesrapport wordt een aanzet gedaan voor zo'n beoordelingsprocedure.

AANBEVELING 5.2

ERBI's wordt aangeraden hun besluiten goed gedocumenteerd vast te leggen en toegankelijk te maken voor onderzoekers en voor andere ERBI's. Op termijn verdient het de aanbeveling te werken aan een goed georganiseerde gezamenlijke opslag waarin alle beslissingen te raadplegen zijn. Deze centrale opslag van 'moresprudentie' biedt de mogelijkheid tot het checken van consistentie en convergentie van beoordelingen en draagt bij aan de vorming van een meer eensluidend beoordelingskader.

CONCLUSION 5.1

Ethicists use ethical value types to articulate the arguments advanced in the process of ethical assessment. Examples of value types are 'respect', 'privacy' and 'wellbeing'. There are many different and divergent values that cannot be reduced to a single type, however. Values do not, furthermore, fit into neat classifications, and they may even conflict with one another. This is equally true of the values common in informatics research. This 'value pluralism' means that it is impossible to provide an unambiguous, unchanging review mechanism. Assessments will have to be made on a case-by-case basis.

CONCLUSION 5.2

The protocols and guidelines for ethical assessment currently used by many Dutch and foreign organisations are relatively limited in scope. The questions they pose generally concern the ethical aspects of identifiable research subjects. They rarely address the effects of research on society or the environment in terms of their ethical dimensions.

RECOMMENDATION 5.1

ERBIs are advised to develop an efficient and transparent procedure that distinguishes between a lenient and a more stringent assessment. The lenient procedure is meant for proposals that concern more standard research. The present advisory report outlines a possible review procedure of this kind.

RECOMMENDATION 5.2

ERBIs are advised to document their opinions properly and to make them available to researchers and other ERBIs. In the longer term, the committee recommends working to build a well-organised, shared repository where all decisions are available for perusal. Having a central repository of 'ethical case law' makes it possible to check for consistency and convergence between reviews and will help to construct a more uniform review mechanism.

Installing ERBIs and developing a shared review mechanism are important steps forward, but they are not enough. It is very important that all researchers become and remain aware of the ethical and legal aspects of their actions. Review boards and the governing bodies of institutions must not take responsibility away from individual researchers. University faculties must nurture a culture in which it becomes 'normal' to think about and discuss these subjects. To do this, they could consider:

- talking about ethical and legal dilemmas during regular and bilateral meetings;
- drafting a code of conduct or making practical agreements in this respect;
- appointing an ethics adviser;
- making training in ethics and integrity a compulsory part of a researcher's education.

Het instellen van ERBI's en het verder ontwikkelen van een gezamenlijk beoordelingskader zijn belangrijke stappen voorwaarts maar niet voldoende. Het is van groot belang dat alle onderzoekers zich bewust zijn en blijven van de ethische en juridische aspecten van hun handelen. Commissies en instellingsbesturen mogen niet de verantwoordelijkheid wegnemen bij de individuele onderzoekers. Aan de faculteiten moet daarom een cultuur ontstaan waarin het 'gewoon' is om over deze onderwerpen na te denken en te discussiëren. Om dit te bevorderen kan worden gedacht aan:

- Praten over ethische en juridische dilemma's in reguliere bijeenkomsten en bilaterale (jaar)gesprekken.
- Opstellen van een gedragscode of het maken van praktische afspraken in dit opzicht.
- Het aanstellen van een ethisch adviseur.
- Ethiek en integriteit verplicht onderdeel maken van de opleiding tot onderzoeker.

CONCLUSIE 6.1

Informaticaonderzoek en de context waarin dit wordt uitgevoerd is continu in beweging. Hierdoor doen zich rondom onderzoeksprojecten voortdurend nieuwe ethische en juridische vraagstukken voor. Eenmalig beoordelen van deze vraagstukken door een beoordelingscommissie bij de aanvang van een project is daarom niet voldoende. Onderzoeksinstituten en individuele onderzoekers moeten constant werken en uitvoering geven aan ethische bewustwording en beoordeling en dit duurzaam verankeren in de organisatie.

CONCLUSION 6.1

Informatics research, and the context in which it is conducted, are in a continuous state of transition. As a result, new ethical and legal issues are constantly arising in relation to research projects. It is not enough to have a review board conduct a one-off review of these issues at the start of a project. Research institutes and individual researchers must work constantly on raising ethical awareness and conducting ethical reviews and make these an inherent part of the organisation.

INHOUD

1. INLEIDING

1.1 Aanleiding voor dit advies

Het initiatief voor dit advies is genomen door de KNAW Adviesraad voor de Technische Wetenschappen, Wiskunde, Informatica, Natuur- en Sterrenkunde en Scheikunde (TWINS). De informatici in deze raad constateren dat onderzoekers in dit vakgebied steeds vaker aanlopen tegen ethische en juridische dilemma's.[1] Bovendien worden de vraagstukken als steeds complexer ervaren. Zowel de samenleving als ook onderzoeksfinanciers verwachten ook meer en meer een gedegen ethische afweging van de wetenschappers en een onderzoeksaanpak die rechtmatig is. Voor onderzoeksvoorstellen die worden ingediend bij het Europese Horizon 2020 programma geldt bijvoorbeeld dat '*A proposal which contravenes ethical principles or any applicable legislation may be excluded from evaluation, selection and award procedures at any time*'.

Momenteel wordt in veel gevallen een ethische of juridische afweging al dan niet expliciet door de betreffende onderzoekers zelf gemaakt. Bij een aantal instellingen wordt echter in navolging van medische, sociale en gammafaculteiten ook geëxperimenteerd met ethische commissies die onderzoeksvoorstellen beoordelen. Dit is een toe te juichen ontwikkeling, maar het is duidelijk dat deze ontwikkeling nog in

1 In dit rapport worden de termen 'ethisch', 'integer' en 'juridisch' gebruikt. De gemeenschappelijke noemer van deze termen is dat het gaat over 'behoorlijk gedrag', anders gezegd 'zoals het hoort'. Uiteraard is er onderscheid in de zin dat over ethisch handelen en in mindere mate over integer handelen discussie kan bestaan en over juridisch handelen veel minder, aangezien bij dat laatste sprake is van vastgelegde regels en wetten. Tegelijkertijd kan ook over de interpretatie en toepassing van regels en wetten gediscussieerd worden. Het gaat er in alle gevallen om dat onderzoekers zelf nadenken over hun gedrag (in vaak nieuwe situaties) en in het ene geval kan er meer dan in het andere geval houvast aan wetten, regels, jurisprudentie of een gedragscode gevonden worden.

de kinderschoenen staat. De komende jaren zal er een beoordelingscultuur moeten groeien waarover binnen het vakgebied consensus bestaat en een beoordelingskader dat transparant en herkenbaar is voor zowel de onderzoeksgemeenschap als de buitenwereld. Bovendien moet worden gezocht naar een manier van beoordelen die enerzijds recht doet aan ethische en juridische kaders, maar tegelijkertijd efficiënt en zonder al te veel bureaucratie kan werken. Het is van groot belang om hier snel mee te starten en niet te wachten tot een concrete aanleiding tot actie dwingt. Met dit advies wil de KNAW een bijdrage leveren aan de ontwikkeling en inbedding van een ethisch en juridisch beoordelingskader in het informaticaonderzoeksgebied.

1.2 Opdracht en samenstelling van de commissie

Voor dit advies heeft het bestuur van de KNAW de Commissie Ethische, Juridische en Veiligheidsaspecten van big data en Informaticaonderzoek ingesteld. Deze commissie bestond uit de volgende personen:

- Prof. dr. Jan Willem Klop (voorzitter), Vrije Universiteit Amsterdam en Centrum Wiskunde & Informatica
- Prof. dr. Jan Bergstra, Universiteit van Amsterdam
- Prof. dr. Frank van Harmelen, Vrije Universiteit Amsterdam
- Prof. dr. Jeroen van den Hoven, Technische Universiteit Delft
- Prof. dr. Bart Jacobs, Radboud Universiteit Nijmegen
- Prof. mr. Corien Prins, Universiteit van Tilburg
- Drs. Melle de Vries, KNAW

Ir. Arie Korbijn (senior beleidsmedewerker KNAW) was secretaris van de commissie.

Opdracht

De commissie had bij de start als taak een kader te schetsen waarbinnen ethische, juridische en veiligheidsaspecten van informaticaonderzoek en daaraan gerelateerd onderzoek kunnen worden beoordeeld (zie bijlage 1). Hierbij werd in de eerste plaats gedacht aan:

- de beoordeling van onderzoek naar de beveiliging van netwerken, computersystemen en de toegang daartoe;
- het verzamelen en gebruiken van grote, vaak privacygevoelige gegevensverzamelingen (big data) zoals die in tal van wetenschapsgebieden in opkomst zijn.

Bij het opstellen van de taakopdracht was al duidelijk dat de vraagstelling erg breed was. Het KNAW bestuur had de commissie daarom verzocht om eerst de contouren

van een mogelijk advies te verkennen en indien nodig het onderwerp in te perken. Na uitgebreide discussie heeft de commissie geconcludeerd dat deze vraagstelling inderdaad te breed is voor een voldoende gericht advies. De ethische en juridische aspecten die te maken hebben met het verzamelen en gebruiken van grote gegevensverzamelingen (big data) over de hele breedte van het wetenschapsveld is een zo omvangrijk – en belangrijk – onderwerp dat een afzonderlijk adviestraject hiervoor gerechtvaardigd is. Bovendien is de doelgroep van een advies over big data veel groter en heterogener dan een advies over vraagstukken die meer beperkt zijn tot de informaticaonderzoeksgemeenschap. De commissie heeft in overleg met het bestuur de opdracht daarom beperkt tot de volgende vraagstelling:

Geef aan hoe informaticaonderzoek beoordeeld kan worden op ethische en juridische aspecten.

Ethische en juridische aspecten van big data die specifiek betrekking hebben op informaticaonderzoek worden uiteraard wel in dit advies meegenomen.

Overigens valt een rigide onderscheid tussen ethische en juridische aspecten niet te maken. Waar juridische aspecten betrekking hebben op in recht verankerde (in wetgeving, jurisprudentie of gedragscodes) en in regels geëxpliciteerde normen en waarden, hebben ethische aspecten onder meer betrekking op juist deze normen en waarden. Bovendien werkt wet- en regelgeving deels met zogenaamde open normen, wat – gegeven de context – noodzaakt tot een nadere interpretatie. Deze interpretatie is mede ingegeven vanuit de normen en waarden die vanuit de ethiek worden aangedragen.

De oorspronkelijke opdracht voor deze commissie spreekt van: ethische, juridische en veiligheidsaspecten van informaticaonderzoek. Het onderwerp veiligheidsaspecten is weggelaten uit de formulering die de commissie zelf hanteert. Hiervoor is gekozen omdat veiligheidsaspecten geen aparte categorie rechtvaardigen en goed als onderdeel van ethische aspecten beschouwd kunnen worden. Daarbij gaat het in het informaticaonderzoek dat hier in de voorbeelden aan de orde komt vooral om beveiliging (*security*) en minder om veiligheid (*safety*). Voor het bredere onderwerp big data heeft de KNAW inmiddels een aparte commissie big data ingesteld.

Doelgroepen

Dit rapport is voor verschillende doelgroepen interessant. In de eerste plaats is het bedoeld voor wetenschappers in informatica en informatie- en communicatietechnologie (ICT). Ethische en juridische dilemma's spelen op alle niveaus. Dit advies is daarom zowel op onderzoeksleiders als op onderzoekers (in opleiding) gericht. Met

dit advies hopen we iedereen die betrokken is bij de advisering over of beoordeling van ethische en juridische aspecten van voorgenomen onderzoeksprojecten een handreiking te geven. In hoofdstuk 4 pleit de commissie voor het instellen van ethische review commissies. Met dit advies hopen we in het bijzonder de leden van dergelijke commissies op weg te helpen.

In de tweede plaats is dit advies bedoeld voor bestuurders in de academische wereld, bijvoorbeeld sectie- of afdelingshoofden, faculteitsbestuurders en leden van colleges van bestuur.

Onderzoekers en onderzoeksleiders moeten dagelijks keuzes maken over een richting en uitvoering van specifieke onderzoeksprojecten. Politieke keuzes hebben regelmatig invloed op de keuzevrijheid van onderzoekers en kunnen ook tot ethische en juridische dilemma's leiden. Agenderen en bewustwording speelt een belangrijke rol. Dit rapport kan daarom ook van belang zijn voor de politiek.

Last but not least richt dit advies zich op het algemene publiek. Uiteindelijk is de maatschappij de ontvanger van de opbrengsten, maar ook van de risico's en gevaren van ontwikkelingen als besproken in dit rapport. Dit rapport is daarom ook voor een algemeen publiek relevant; en daarmee voor vertegenwoordigers van media zoals wetenschapsjournalisten en anderen die een intermediaire functie vervullen tussen wetenschap en publiek.

Afbakening onderzoeksgebied

De commissie heeft zich geconcentreerd op de dilemma's die spelen bij onderzoek zoals dat wordt uitgevoerd aan de Nederlandse Informatica-afdelingen en onderzoeksinstituten. Daarbij is er een aantal subdomeinen waar de meeste ethische en juridische kwesties spelen. Daarbij moet gedacht worden aan de volgende gebieden:

- *computer security, data security, cryptography;*
- *data mining, machine learning, data science;*
- *robotics, drones, autonomous systems;*
- *human-computer interaction, gaming;*
- *reliability, software quality;*
- *web technology;*
- *wearable computing, internet of things, embedded computing.*

Deze lijst is verkregen door een rondgang van de commissie langs de Nederlandse instellingen en universiteiten.

Nota Bene: in bovenstaande afbakening van gebieden komen ook aan big data gerelateerde onderzoeksthema's voor, zoals in *data-mining*, *machine learning*, *wearable computing* enz. Met onze afbakening willen we dit onderzoek beslist niet uitsluiten. De boven beschreven gebiedsafbakening betreft wel de uitsluiting van big data in zijn volle omvang, waar tal van andere aspecten en gebieden aangetroffen worden, met name sociologische inclusief sociale media [Dijck, José van, 2013 en 2014], economische [Davenport, 2014, Davis, 2012, Lohr 2015a en b], commerciële (zie bijv. [Tanner 2014]) en maatschappij-kritische [Morozov, 2013].

1.3 Werkwijze

De commissie heeft op verschillende manieren informatie verzameld en geanalyseerd. Door middel van interviews met een aantal sleutelfiguren uit het informaticaonderzoek (zie bijlage gesprekspartners en referenten) heeft de commissie zich allereerst een beeld gevormd van de manier waarop aan de verschillende instellingen tegen dit onderwerp wordt aangekeken, of en zo ja hoe onderzoek wordt beoordeeld en welke dilemma's en knelpunten men ervaart. Voor het beoordelingskader is een groot aantal protocollen en documenten van Nederlandse en buitenlandse instellingen geanalyseerd. De commissie heeft meerdere keren vergaderd en op basis van de verzamelde informatie en eigen deskundigheid een advies op hoofdlijnen opgesteld. De contouren van dit advies zijn op 15 juni 2015 gepresenteerd tijdens een klankbordbijeenkomst in het Trippenhuis in Amsterdam. Uit deze bijeenkomst bleek draagvlak voor de hoofdlijn van dit advies. Wel maken sommige deelnemers zich zorgen over het ontstaan van teveel bureaucratie. De commentaren van deze bijeenkomst zijn meegenomen in de definitieve versie van dit advies. Volgens de gebruikelijke werkwijze van de KNAW is het rapport *gereviewd* door externe *reviewers* (zie bijlage gesprekspartners en *reviewers*). Deze commentaren zijn vervolgens door de commissie verwerkt.

2. ETHISCHE EN JURIDISCHE DILEMMA'S BIJ INFORMATICAONDERZOEK

2.1 Inleiding

Traditioneel worden informatici gezien als de architecten van de digitale wereld. In de afgelopen decennia is duidelijk geworden dat zij ook mede de architecten en vormgevers van de sociale wereld zijn. Een groot deel van onze sociale interactie verloopt inmiddels via elektronische middelen. De inrichting van deze middelen, de controle daarover, en de controle over het berichtenverkeer, zijn cruciaal voor de sociale en maatschappelijk ordening. Het adagium 'kennis is macht' is verruimd tot 'informatie is macht'. Daarmee hebben de technische beslissingen die informatici nemen bij het ontwerpen en bouwen van computersystemen vaak directe ethische, maatschappelijke en politieke consequenties. Dit brengt een aanzienlijke verantwoordelijkheid met zich mee en roept nieuwe vragen op.

Is het bijvoorbeeld wenselijk dat informatici onderzoek doen naar betere algoritmen voor privacybescherming? Moeten ze wel een commerciële opdracht aannemen om hun *machine learning* software te optimaliseren voor het herkennen of uitsluiten van bepaalde groepen (verdachten, meer of juist minder draagkrachtigen, etc)? Moeten ze expliciet op zoek gaan naar fouten of kwetsbaarheden in bestaande software, en zo ja, wat moeten ze doen bij het aantreffen daarvan? In hoeverre mogen ze faciliteren dat met behulp van programmatuur bepaalde (voor het publieke domein dan wel publieke debat relevante) informatie – om commerciële dan wel andere redenen – achter een digitaal slot wordt gezet? Welke verantwoordelijkheid hebben zij om proactief over deze en vergelijkbare vragen na te denken en er aandacht op te vestigen?

De term ‘informaticus’ wordt hier gebruikt ter aanduiding van een academische onderzoeker op het gebied van de informatica of van een aanverwant vakgebied (informatiekunde, kunstmatige intelligentie, wiskunde, mogelijk zelfs delen van bestuurskunde of rechten). Zo’n onderzoeker zal typisch bij een universiteit of instelling voor hoger onderwijs in dienst zijn, maar mogelijk ook bij een (semi)publieke of private organisatie waar een redelijke mate van vrijheid van onderzoek bestaat. De term ‘gegevens’ wordt in het onderstaande in ruime zin gebruikt, dat wil zeggen ter aanduiding van niet alleen gegevens in de strikte zin van het woord, maar ook omvattende software, informatie, en metadata die met behulp van gegevens worden gegenereerd.

2.2 Typerende voorbeelden van dilemma’s

Veiligheid van computersystemen is een belangrijk onderzoeksonderwerp binnen de informatica. De ontwikkelingen op dit terrein gaan snel. Dit geldt ook voor het vernuft van groepen die te kwader trouw toegang trachten te krijgen tot deze systemen. Voor het vergroten van de kennis van dit soort beveiligingsvraagstukken is het ook nodig om te weten hoe deze mensen werken. Aan dit soort onderzoek kleven tal van ethische en juridische vragen. We zullen dit aan de hand van een paar voorbeelden illustreren. Zie ook de praktijkvoorbeelden in [CBP, 2013].

Pobelka-botnet

Een botnet is een netwerk van geïnfecteerde computers dat gebruikt kan worden voor criminele activiteiten zoals het verzamelen en voor misbruik ter beschikking stellen van codes voor digitaal betalingsverkeer. Een bekend voorbeeld hiervan is het Pobelka-botnet dat eind 2012 door twee Nederlandse beveiligingsbedrijven werd ontmanteld. Via dit netwerk werd minstens 750 GB aan informatie gestolen, onder andere van zo’n 150.000 Nederlandse computers. Het beveiligingsbedrijf Digital Investigation wist 750 GB aan informatie te achterhalen die de aanvallers van de besmette pc’s hadden buitgemaakt. Het gaat hierbij onder andere om gegevens over de computernetwerkstructuur van een grote multinational, lopende zaken van een gerenommeerd advocatenkantoor en komende rechtszaken, productontwikkeling van een technologisch vooraanstaand bedrijf, welke medewerker op een ministerie precies aan welke Kamervragen werkt, de informatie die op diverse krantenredacties circuleert.

Vanuit onderzoeksoogpunt zijn deze gegevens bijzonder interessant. Ze kunnen immers veel inzicht geven in de manier waarop zo’n botnet functioneert en over de manier waarop dit fenomeen bestreden kan worden. In ingewikkelde gevallen zijn onderzoekers soms ook betrokken bij de daadwerkelijke ontmanteling van dit soort kwaadaardige netwerken. De vraag of je gebruik mag maken van deze gegevens, heeft

echter tot veel discussie geleid. In hoeverre is dit juridisch en ethisch geoorloofd? Mag je gegevens die overduidelijk van diefstal afkomstig zijn überhaupt bewaren en gebruiken voor wetenschappelijk onderzoek? Heiligt het doel hier de middelen? Meer in het algemeen speelt de vraag in hoeverre je bij bepaalde inbreukmakende handelingen op het internet betrokken wordt als het observeren van dergelijke handelingen een wezenlijk onderdeel van je onderzoek is. Bijvoorbeeld onderzoek naar illegaal, strafbaar of ander onrechtmatig gedrag op internet (kinderporno, illegaal downloaden, etc.).

Mifare Classic Chip en Megamos-crypto-algoritme in startonderbrekers van Volkswagen

De firma NXP brengt sinds 1995 de Mifare Classic Chip op de markt. Deze chips worden zeer veel toegepast in beveiligings- en transportsystemen. Zo wordt de chip onder meer gebruikt in de Nederlandse OV-chipkaart en in miljoenen toegangspassen voor gebouwen en terreinen van bedrijven en instellingen, waaronder de Nederlandse overheid. De chip communiceert via radiosignalen contactloos met ontvangers die bijvoorbeeld in toegangspoortjes zijn aangebracht. Om de communicatie te beveiligen en misbruik te voorkomen wordt de informatie versleuteld via een geheim algoritme, het zogenaamde CRYPTO-1-algoritme. Onderzoekers van Radboud Universiteit Nijmegen ontdekten in maart 2008 een lek in de beveiliging van deze chip waardoor zij in staat waren de werking van het CRYPTO-1-algoritme te doorgronden en op een betrekkelijk eenvoudige manier de cryptografische sleutels te achterhalen. Door deze twee punten te combineren kon een toegangspas succesvol worden gekloond.

Zoals gebruikelijk in het securityonderzoek hebben de betreffende onderzoekers via een *responsible disclosure* (zie voor uitleg het Glossarium) de fabrikant van de chips op de hoogte gesteld. Omdat de chip in tal van (overheids) systemen en in de OV-chipkaart wordt gebruikt zijn ook de overheid en belangrijke gebruikers geïnformeerd. Daarbij hebben de onderzoekers ook gemeld de resultaten te gaan publiceren in de conferentiebundel van de ESORICS-conferentie, met inachtneming van een periode om NXP de gelegenheid te geven maatregelen te nemen.

Voor NXP was dit aanleiding de rechter te vragen deze publicatie te verbieden op straffe van een dwangsom van 1 miljoen euro. Ook werd geëist dat de onderzoekers alles in het werk zouden stellen om geheimhouding door de organisatoren van de conferentie en de *reviewers* te bewerkstellingen. NXP beriep zich hiertoe op een inbreuk op haar intellectuele eigendomsrechten hetgeen een onrechtmatige daad oplevert. De Rechtbank van Arnhem wees deze claim echter af. De rechter vond dat onvoldoende was aangetoond dat het algoritme van de chip een auteursrechtelijk beschermd werk is of voor geschriftenbescherming in aanmerking kon komen. Bovendien had NXP

onvoldoende duidelijk kunnen maken waarom het recht op publicatie moest worden beperkt [Rechtspraak.nl, NJ 2008, 544 , Computerrecht 2008, 140 met annotatie van S.F.E. Verdonck].

Buitenlandse rechters oordelen in vergelijkbare zaken echter soms anders. Onderzoekers van dezelfde Nijmeegse onderzoeksgroep ontdekten in 2012 kwetsbaarheden in het zogenaamde Megamos-crypto-algoritme dat wordt gebruikt in de elektronische startonderbrekers van verschillende automerken, waaronder Volkswagen. Ook deze zwakke plek werd volgens een *responsible disclosure* gemeld aan het Zwitserse bedrijf EM Microelectronic. Toen Volkswagen vernam van het voornemen tot publicatie besloot zij de rechter te vragen om een verbod. Omdat de eerste auteur van het artikel inmiddels werkzaam was in het Verenigd Koningrijk werd de zaak aanhangig gemaakt in Londen. Volkswagen betoogde dat de publicatie de diefstal van miljoenen auto's in de hand zou werken. In juni 2013 stelde de Londense rechtbank Volkswagen in het gelijk en werd de onderzoekers verboden te publiceren. Het belang van Volkswagen woog volgens de rechter zwaarder dan de vrijheid van publicatie. Dit verbod is twee jaar van kracht geweest en is pas na tijdrovende en langdurige onderhandelingen opgeheven [Mols, 2013, Hof, van 't, 2015].

Onderzoek naar effectiviteit van blokkades van The Pirate Bay

The Pirate Bay is een van de meest bekende websites voor het onderling delen van, meestal auteursrechtelijk beschermde, bestanden. Via deze site kunnen gebruikers eenvoudig muziek, films of games met elkaar delen. De in 2003 in Zweden opgerichte website stond in 2013 in de top-100 van meest bezochte websites. Door een krachtige lobby van de entertainment industrie is wereldwijd geprobeerd om de activiteiten van deze site aan banden te leggen. In Nederland heeft de stichting Brein met juridische middelen geprobeerd om internetproviders te dwingen de toegang tot The Pirate Bay te blokkeren. Op 11 januari 2012 werden zij door de rechtbank in Den Haag in het gelijk gesteld en werden de providers Ziggo en XS4ALL verplicht om de toegang tot The Pirate Bay te blokkeren. De providers hebben hier onder protest gehoor aan gegeven.

Gezien het dynamische karakter van internet werd door deskundigen verwacht dat deze blokkades weinig effect zouden hebben omdat gebruikers vrij snel manieren zouden vinden om de blokkades te omzeilen. Er was echter nooit wetenschappelijk onderzoek gedaan naar het effect van blokkades. Gedegen kennis van het effect van zo'n blokkade is van belang voor bijvoorbeeld Internet Society Netherlands maar ook voor beide partijen in het conflict. Onderzoekers van de Universiteit van Amsterdam hebben daarom een gereedschap ontwikkeld om de effectiviteit van deze blokkades te kunnen meten. Dit gereedschap verzamelt gegevens van de Pirate-Bay-website waaronder IP-adressen van individuele gebruikers. De gegevens die hierdoor worden

verzameld zijn daarom privacygevoelig en bovendien verkregen van een website waarvan de handelwijze juridisch en ethisch gezien discutabel is.

Grindr

Grindr (http://grindr.com) is een geosociale applicatie (app) voor smartphones, bedoeld om homoseksuele mannen met elkaar in contact te brengen. Door middel van geolocatie kunnen gebruikers van Grindr zien welke mannen zich in de omgeving bevinden. Deze worden in de user interface getoond door middel van kleine profielfotootjes, die gerangschikt zijn van dichtbij naar ver weg. Door het fotootje van een andere gebruiker aan te klikken, verschijnt een kort profiel en de mogelijkheid om te chatten, foto's te versturen of de eigen locatie door te geven.

Grindr werd op 25 maart 2009 gelanceerd door het Amerikaanse bedrijf Nearby Buddy Finder, LLC. Het werd al snel wereldwijd gebruikt en op 18 juni 2012 maakte Grindr bekend dat er 4 miljoen gebruikers in 192 landen waren, waarvan 1,1 miljoen dagelijks online waren. Ruim 1,5 miljoen gebruikers bevinden zich in de Verenigde Staten en met 350.000 is Londen de stad met de meeste gebruikers. In Nederland zijn er ca. 15.000 gebruikers van Grindr.

Studenten van de System and Network Engineering research group van de Universiteit van Amsterdam vonden in het kader van een van de studieopdrachten een lek in deze smartphone-applicatie. Hierdoor waren ze in staat om de achterliggende database te benaderen en de data te manipuleren. Gezien de aard van deze applicatie betrof dit uiterst privacygevoelige informatie. Dit lek is gemeld aan Grindr volgens een *responsible disclosure* (voor uitleg zie het Glossarium).

2.3 Wat kunnen we leren van bijvoorbeeld toetsing van medisch onderzoek?

In de *Wet Mensgebonden Onderzoek* (WMO) is vastgelegd dat medisch-wetenschappelijk onderzoek met mensen moet worden beoordeeld door een onafhankelijke commissie van deskundigen. Onderzoek valt onder de WMO als aan de volgende twee voorwaarden is voldaan:

1. er is sprake van medisch-wetenschappelijk onderzoek, en
2. personen worden aan handelingen onderworpen of aan hen worden gedragsregels opgelegd.

Het doel van de WMO is overigens alleen de bescherming van proefpersonen. Dit betekent dat alleen hun belangen afgewogen hoeven te worden en er geen brede afweging

van allerhande ethische aspecten gemaakt hoeft te worden. Medische handelingen die in het kader van patiëntenzorg worden verricht vallen ook niet onder de WMO en hoeven ook niet aan een toetsingscommissie te worden voorgelegd. Een positief oordeel is nodig voordat met een onderzoek gestart mag worden. Er zijn in Nederland twee typen commissies, de Centrale Commissie Mensgebonden Onderzoek (CCMO) en 24 regionale erkende medisch-ethische toetsingscommissies (METC). De meeste zijn verbonden aan een instelling, zoals een universitair medisch centrum of een ziekenhuis. Juridisch zijn deze commissies echter een zelfstandig bestuursorgaan (ZBO) en daarmee juridisch onafhankelijk.

De METC's beoordelen het meeste medische-wetenschappelijke onderzoek. Vrijwel alle onderzoek met wilsbekwame volwassenen valt onder de METC's evenals het therapeutisch onderzoek en het niet-therapeutisch observationeel onderzoek met minderjarigen en wilsonbekwame volwassenen. Voor bepaalde typen onderzoek is bij wet bepaald dat een bundeling van de expertise in één commissie noodzakelijk is, dit is de CCMO. Het gaat daarbij om de beoordeling van onderzoek met specifieke of specialistische ethische, juridische of maatschappelijke aspecten. Dit is bijvoorbeeld het geval bij onderzoek op het gebied van celtherapie, xenotransplantatie, onderzoek met stamcellen. Voor meer informatie zie www.ccmo.nl.

Eisen aan een METC

Alleen erkende METC's mogen onderzoek beoordelen. Om voor erkenning in aanmerking te komen moet onder andere voldaan worden aan wettelijke eisen omtrent de samenstelling van de commissies, deskundigheid van de leden, werkwijze en minimum aantal beoordelingen per jaar (zie tabel 2.1 hiernaast).

Beoordelingsgronden

In de WMO is vastgelegd dat een ethische commissie alleen een positief oordeel kan geven over een onderzoeksprotocol als voldaan is aan een aantal voorwaarden. Zo moet bijvoorbeeld aannemelijk worden gemaakt dat het voorgestelde onderzoek tot nieuwe medische inzichten kan leiden en dat het niet door andere minder ingrijpende vormen van wetenschappelijk onderzoek kan gebeuren. Ook worden er eisen gesteld aan het personeel dat de proeven uitvoert en moeten de belangen van de proefpersonen voldoende worden gewaarborgd.

Tabel 2.1 Wettelijke eisen aan Medisch-Ethische Toetsingscommissies (Bron: Wet Medisch onderzoek, artikel 16).

Eisen voor een erkende METC	Toelichting
Samenstelling	Moet minimaal bestaan uit: één of meer artsen, een jurist, een ethicus, een onderzoeksmethodoloog en iemand die vanuit het perspectief van een proefpersoon kan kijken. Indien de commissie ook geneesmiddelenonderzoek beoordeelt moet er daarnaast nog een ziekenhuisapotheker en een klinisch farmacoloog in de commissie zitten (mag in één persoon verenigd zijn).
Reglement	Er is een reglement wat voorziet in minimaal aantal vereisten over onafhankelijkheid, etc.
Werkwijze	De werkwijze van de METC is goed geregeld en omschreven.
Externe deskundigen	Een commissie moet externe deskundigheid kunnen aantrekken als het te beoordelen onderzoek daarom vraagt.
10-protocollen-eis	Het moet in de lijn der verwachting liggen dat een commissie jaarlijks minimaal tien voorstellen beoordeelt.

Praktijk

Samengevat werkt de toetsing van medisch ethisch wetenschappelijk onderzoek in de praktijk als volgt:

- onderzoeker beoordeelt of onderzoek WMO-plichtig is
- zo ja, dient deze een onderzoeksprotocol in bij METC of CCMO
- die beoordeelt op grond van:
  - ontvankelijkheid
  - voorschriften wet (m.n. wilsonbekwamen)
  - afweging belasting en voordeel voor individu of groep

De focus van deze afweging ligt vooral op de gevolgen voor de proefpersonen. Wat bijvoorbeeld niet wordt gewogen zijn:

- groepseffecten
- risico's voor maatschappij
- risico's van een behandeling

Bruikbaarheid van deze ervaring bij informaticaonderzoek

Door de sterke focus op de gevolgen voor proefpersonen zijn de ervaringen met medische ethische toetsing slechts beperkt bruikbaar bij informaticaonderzoek. Bij veel informaticaonderzoek zijn immers geheel geen proefpersonen betrokken terwijl er wel specifieke ethische dilemma's aan zijn verbonden. Bovendien bestaat er geen wettelijke verplichting om informaticaonderzoek aan een ethische commissie voor te leggen. De eisen die wettelijk aan een METC worden gesteld voor wat betreft samenstelling, werkwijze en reglement kunnen wel bruikbaar zijn bij het opzetten van ethische toetsingscommissies binnen de informatica (zie hoofdstuk 4).

2.4 Conclusies

CONCLUSIE 2.1

In de maatschappij in brede zin, maar ook in het bijzonder door onderzoeksfinanciers, wordt meer en meer een gedegen ethische afweging van wetenschappers gevraagd. Dit geldt voor veel vakgebieden maar zeker voor de informatica gezien de enorme maatschappelijk effecten en het belang van dit vakgebied. Het is gewenst dat er binnen dit vakgebied een morele infrastructuur wordt ontwikkeld. Dit betekent dat er een transparant en herkenbaar beoordelingskader moet groeien waarover binnen het vakgebied consensus bestaat. Bovendien moet worden gezocht naar een manier van beoordelen die zorgvuldig en gedegen, maar tegelijkertijd ook efficiënt is en zonder al te veel bureaucratie kan werken.

CONCLUSIE 2.2

In de medische wetenschappen is al veel ervaring opgedaan met ethische beoordeling van onderzoek. Door de sterke focus op de gevolgen voor proefpersonen is die ervaring niet één op één te gebruiken in het geval van informaticaonderzoek. Aan informaticaonderzoek kleven ethische vraagstukken met een geheel eigen karakter. Bovendien ontbreekt bij informaticaonderzoek een wettelijke verplichting op ethische toetsing. Het vakgebied zal daarom met gebruik van de ervaringen uit de medische disciplines zelf een eigen toetsingskader en manier van toetsing moeten ontwikkelen.

3. JURIDISCHE ASPECTEN

3.1 Inleiding

In informaticaonderzoek is met grote regelmaat sprake van het verzamelen of bewerken van persoonsgegevens, alsmede van onderzoek gedaan naar software of computersystemen waarvan de eigendomsrechten bij anderen liggen. Hierdoor zitten aan dit type onderzoek al snel juridische vragen met betrekking tot bijvoorbeeld privacy of intellectuele eigendomsrechten. Dit rapport ambieert niet gedetailleerd in kaart te brengen wat juridisch gezien wel of niet toegestaan is en onder welke voorwaarden en omstandigheden dat het geval is. Die insteek ligt buiten de opdracht van de commissie. Bovendien hangt de concrete uitkomst van het toepasselijk wettelijk kader sterk van de context af en moet daarom in voorkomende gevallen meestal juridische expertise worden ingeroepen. Wel willen we in dit hoofdstuk op hoofdlijnen een beeld schetsen van de belangrijkste juridische voorwaarden voor en implicaties van informaticaonderzoek. Dat doet de commissie onderstaand door de verschillende stadia van dit onderzoek te beoordelen op de implicaties vanuit intellectuele eigendomsrechten en privacy.

De commissie beseft dat de relevante wet- en regelgeving meer omvat dan uitsluitend het regelgevend kader binnen deze twee domeinen – te denken valt aan aansprakelijkheid, computercriminaliteit, wettelijke bepalingen inzake beveiliging en integriteit van systemen. Zowel kwesties rondom intellectuele eigendomsrechten als aandacht voor privacybescherming vragen in onze ogen echter bij voorrang aandacht en zullen bovendien in vrijwel alle situaties relevant blijken te zijn. Wel wordt aan het slot van dit hoofdstuk kort stilgestaan bij een bijzondere verantwoordelijkheid die vanuit de wet en rechtspraak aan onderzoekers wordt opgelegd, namelijk de zorgplicht. Het gaat dan bijvoorbeeld om de vraag in welke situaties informatieonderzoekers de plicht

hebben om verdachte of ongebruikelijke patronen niet links te laten liggen. Gedacht kan bijvoorbeeld worden aan kennis die tijdens eigen onderzoek wordt verkregen over misbruik door derden van een beveiligingslek. Zo heeft de Amerikaanse NSA jarenlang gebruik gemaakt van een internetbeveiligingslek genaamd *Heartbleed*. In plaats van het bij relevante partijen te melden, zodat deze de nodige aanpassingen in de systemen konden doorvoeren, bleef men heimelijk door de opening meegluren en schond daarmee wereldwijd de privacy van velen. De NSA is zeker niet de enige die misbruik maakt van beveiligingslekken. Er is een commerciële markt voor zgn. *zero-day exploits*. Kort samengevat is een *zero-day exploit* een software-applicatie die speciaal is ontwikkeld om misbruik te maken van een beveiligingslek bij bijvoorbeeld een internetdienst (zie ook Glossarium). Met behulp van een *zero-day exploit* valt het ICT-systeem binnen te dringen zonder dat de aanbieder van dit systeem daar weet van heeft. Kortom, wie de beschikking heeft over een *exploit* kan heimelijk observeren, gegevens aftappen, virussen installeren, etc. Indien informaticaonderzoekers tijdens hun onderzoek stuiten op een concrete praktijk, zullen ze vanuit een zorgplicht hebben te handelen. Bijvoorbeeld door de aanbieder van het systeem te wijzen op het lek, waarmee deze de kans krijgt een herstelapplicatie voor het lek naar gebruikers te distribueren en de *exploit* niets meer waard is [Prins, 2014; Grossman, 2014]. De vraagstukken op het terrein van zorgplichten treden vooral op bij twee typen onderzoek die zeer gangbaar zijn in dit onderzoeksveld: Onderzoek naar kwetsbaarheden in software en onderzoek met gebruik van gegevensbestanden met privacygevoelige informatie (zie ook de cases in paragraaf 2.2).

3.2 Keuze van het onderzoeksonderwerp

Veel voorkomend onderzoek in de informatica is onderzoek waarbij een computer *security*-onderzoeker de werking van bestaande software onderzoekt. Dit kan gaan om een onderzoek naar de gegevensstromen bij een 'app' op een mobiele telefoon of tablet, om na te gaan welke gegevens van en naar de gebruiker worden gestuurd en naar wie. Ook kan het gaan om onderzoek naar de mate waarin een kwaadwillende de werking kan beïnvloeden van bijvoorbeeld een pacemaker, een bankkaart, een stemcomputer, of van software in een moderne auto.

Een eerste vraag is natuurlijk of een (academisch) informaticus dit soort zaken überhaupt wel moet onderzoeken? Daar lijkt weinig controverse over te zijn. Het maatschappelijke belang van dit soort onderzoek rechtvaardigt in veel gevallen de eventuele negatieve gevolgen voor bedrijven, overheden of individuen. Het kritisch en onafhankelijk onderzoeken van bestaande methoden en technieken komt ook op andere gebieden voor (bijvoorbeeld onderzoek naar bijwerkingen van medicijnen) en kent een lange academische traditie. In sommige gevallen zal de producent van het onderzoeksonderwerp op de hoogte zijn van het onderzoek, maar vaak ook niet.

Een tweede vraag betreft de keuze van het onderzoeksonderwerp. In de academische praktijk is deze keuze vaak een vrij willekeurig proces dat door verschillende aspecten wordt beïnvloed: de persoonlijke interesse of expertise van de individuele onderzoeker, de beschikbaarheid van onderzoeksmiddelen, de wetenschappelijke stand van zaken en daarmee potentiële bijdrage aan wetenschappelijke innovatie, de maatschappelijke of commerciële relevantie, en de toegankelijkheid van de software. In de praktijk richt dit soort kwetsbaarhedenonderzoek zich vaak op software in "kleine" apparaten zoals chipkaarten of telefoons omdat die relatief makkelijk toegankelijk zijn in vergelijking met grote softwaresystemen onder beheer van anderen.

Belangrijke aandachtspunten

Bij een zelfgekozen onderzoeksonderwerp moet altijd de wetenschappelijke of maatschappelijke relevantie goed onderbouwd kunnen worden, zeker omdat bij informaticaonderzoek de niet-wetenschappelijke implicaties van het onderzoek grote betekenis kunnen hebben. In het bijzonder moet duidelijk zijn wie op welke wijze benadeeld of wellicht bevoordeeld wordt bij het falen van de beveiliging van informatie en bij het bekend worden van dit falen. Een eventueel eigenbelang van de onderzoeker of van het instituut waar hij/zij werkt zal expliciet gemaakt moeten worden. De commissie meent dat dit soort onderzoek enkel verricht kan worden wanneer geen sprake is van zulk eigenbelang.

Daarnaast moet voorafgaand aan het onderzoek worden nagegaan of door dit onderzoek mogelijk inbreuk wordt gemaakt op rechten en belangen van derden. Zo kunnen door het doorbreken van beveiliging de privacyrechten of intellectuele eigendomsrechten van anderen dan de producent van het onderzoeksonderwerp worden geschonden. Indien hiervan potentieel sprake is, moet de onderzoeker of het betreffende onderzoeksinstituut een expliciete afweging maken tussen enerzijds het wetenschappelijk en maatschappelijk belang dat is gediend met het onderzoek en anderzijds de rechten van derden die mogelijk worden geschonden. Bij deze afweging moet scherp voor ogen worden gehouden dat het doel niet altijd alle middelen rechtvaardigt. Een te omvangrijke dan wel ingrijpende schending van rechten van derden kan aanleiding zijn om het onderzoek helemaal niet of alleen in gewijzigde vorm uit te voeren. Ook zal de onderzoeker er zorg voor moeten dragen dat aan bepaalde wettelijke voorwaarden wordt voldaan, zoals bijvoorbeeld het adequaat afschermen van de persoonsgegevens die met het onderzoek in beeld komen. Zelfs als een belangenafweging is gemaakt, kan het onderzoek onder bepaalde omstandigheden nog steeds in strijd met het recht zijn. Bijvoorbeeld omdat met het onderzoeken van de software het auteursrecht van de rechthebbende op deze software wordt geschonden.

3.3 Juridische aspecten in verschillende fasen van het onderzoek

In deze paragraaf wordt ingegaan op een aantal kwesties die spelen in de verschillende fasen van het onderzoek en hoe daarmee kan worden omgegaan.

3.3.1 Verwerving en beheer van gegevens

Zodra het onderzoeksonderwerp is bepaald moeten er meestal onderzoeksgegevens worden verzameld. Het verwerven van onderzoeksgegevens kan bij onderzoek van software en dataverzamelingen op verschillende manieren gebeuren. De software kan vrij beschikbaar zijn (als *open source*), tegen betaling, of impliciet bij aankoop van het apparaat waarin de te onderzoeken software zit. In dat laatste geval zijn extra handelingen nodig voor het maken van een *memory dump*, waarbij mogelijk enige beveiliging moet worden doorbroken. Ook kan de software op illegale wijze beschikbaar zijn, bijv. via *pirate*-websites. Lang niet altijd zal direct duidelijk zijn wie de rechthebbende op de software is, en welke rechten van toepassing zijn dan wel welke voorwaarden aan een eventuele licentie zijn verbonden. Mogelijk is er ook sprake van 'gevoelige software' die niet algemeen bekend is. Dit is bijvoorbeeld het geval bij software die gebruikt wordt in bankkaarten. Onderwerpen die in deze fase juridische of ethische dilemma's kunnen veroorzaken zijn: de betrouwbaarheid van bronnen, geheimhouding, anonimisatie, *reverse engineering* en beveiligde opslag. Bij het onderzoeken van software en gegevensverzamelingen worden handelingen verricht die soms zijn aan te merken als een juridisch relevante handeling, bijvoorbeeld een auteursrechtelijk beschermde verveelvoudiging van de software en gegevensverzameling. Het kan zijn dat daarvoor de toestemming van de rechthebbende vereist is. Met de volgende maatregelen wordt de kans op juridische problemen verkleind.

- Documenteer zo helder mogelijk de herkomst van de software en daarmee de rechten die op de software dan wel dataverzameling van toepassing zijn. Indien op de software of dataverzameling een intellectuele eigendomsrecht rust (auteurs-, octrooi- dan wel databankenrecht): beoordeel of het gebruik hiervan mogelijk is op grond van een licentie dan wel een van de wettelijke gebruiksgronden. Overigens is slechts in zeer uitzonderlijke gevallen sprake van dergelijke wettelijk gelegitimeerde gebruiksgronden. Indien nog geen licentie beschikbaar is op grond waarvan het gebruik te rechtvaardigen valt, is het noodzakelijk deze alsnog te verkrijgen.
- Zorg voor versleutelde opslag van gevoelige software, mogelijk op volledig geïsoleerde informatiedragers die niet aan het internet gekoppeld zijn. Zorg ook voor versleutelde communicatie indien verschillende onderzoekers samenwerken, en resultaten en bevindingen bijvoorbeeld per email uitwisselen.

- Beoordeel of als onderdeel van het gebruik ook persoonsgegevens in het geding zijn. Indien dit het geval is, formuleer het doel waarvoor deze gegevens worden gebruikt en draag zorg voor het gebruik van deze gegevens conform de diverse zorgvuldigheidseisen die in de *Wet bescherming persoonsgegevens* worden gesteld.

3.3.2 Bewerking en gebruik van gegevens

De software die in de vorige fase is verworven, is mogelijk nog niet leesbaar voor mensen. In dat geval zal eerst gedecompileerd moeten worden. Dit proces van het inzichtelijk maken van de werking van (software in) een apparaat is een onderdeel van *reverse engineering*. In de *Europese Softwarerichtlijn* is bepaald dat reverse engineering wettelijk slechts in bepaalde gevallen is toegestaan (zie kader 3.1). Kort samengevat komt het erop neer dat:

- *decompilatie/reverse engineering* niet is toegestaan, als dit niet expliciet is toegestaan in de licentie van de software. In het algemeen staan proprietaire licenties dat niet toe.
- observeren, bestuderen en testen wel is toegestaan voor zover dat mogelijk is met handelingen die onder de licentie vallen dan wel met voor het gebruik van het computerprogramma noodzakelijke handelingen waarbij dit programma wordt geladen en uitgevoerd. Dit kan van nut zijn voor onderzoek naar feitelijke gegevensstromen bij een app op een mobiele telefoon (of tablet), om na te gaan welke gegevens van de gebruiker waar naar toe gestuurd worden. Voor veel andere vormen van onderzoek zal waarschijnlijk *decompilatie* nodig zijn en daarvoor biedt art. 5 (3) *EU Softwarerichtlijn* geen basis (even aangenomen dat de licentie dit niet toestaat).
- *decompilatie*/*reverse engineering* is volgens art. 6 van de *Softwarerichtlijn* wel toegestaan ten behoeve van interoperabiliteit mits het zich beperkt tot die delen van een programma die voor interoperabiliteit van belang zijn (de interfaces). Gegeven de beperkte strekking zal deze bepaling niet of nauwelijks van nut zijn voor *security*-onderzoek. Of de bepaling gebruikt zou kunnen worden voor *security*-onderzoek dat zich richt op de veiligheid van interfaces tussen computers is onduidelijk bij gebrek aan rechtspraak rond dit onderwerp.

Een belangrijk deel van deze bewerkingsfase bestaat uit het begrijpen, modelleren, analyseren en testen van de software. Bij het testen kan soms interactie nodig zijn met *live* systemen. Bijvoorbeeld, bij onderzoek naar het communicatiegedrag van een app zal die app mogelijk uitgeprobeerd worden bij een specifieke gebruiker. Daarbij zullen gebruiksopties uitgeprobeerd worden die door de rechthebbende op de software wel of niet voorzien zijn. De eigenaar van de server waarmee de app een verbinding legt kan dit onvoorziene gedrag mogelijk detecteren, en hier op enige manier op reageren die consequenties heeft voor de gebruiker. Een vergelijkbare situatie kan zich voordoen bij een gemanipuleerde bankkaart of OV-chipkaart die bij een

KADER 3.1:
ART. 5(3) EUROPESE SOFTWARERICHTLIJN EN ART. 45I AUTEURSWET

Degene die onder licentie een kopie van een computerprogramma heeft verkregen, kan zonder de toestemming van de auteursrechthebbende de functionaliteit van dit programma observeren, bestuderen of uittesten teneinde vast te stellen welke ideeën en beginselen aan een element van dat programma ten grondslag liggen, wanneer deze persoon door die licentie gedekte handelingen verricht, alsook handelingen waarbij het programma wordt geladen en uitgevoerd en die voor het gebruik van het computerprogramma noodzakelijk zijn, op voorwaarde dat hij geen afbreuk doet aan de exclusieve rechten van de rechthebbende van dit programma.

reguliere kaartlezer gebruikt wordt. Het testen dient zoveel mogelijk in eigen omgeving plaats te vinden, los van de infrastructuur van anderen. Een eventueel contact van de onderzochte software met de *live* omgeving moet alleen plaatsvinden indien daar dwingende redenen voor zijn. Daarbij moet schade aan de omgeving vermeden worden. In het bijzonder mag de onderzoeker op geen enkele manier eigen voordeel bewerkstelligen met eventueel verkregen toegang, of afgeschermde informatie inzien of veranderen. Omdat bij het testen en mogelijk daartoe bewerken van software of databestanden sprake is van een juridische relevante handeling (er is sprake van 'verveelvoudiging' van software dan wel 'ontlening' van data), geldt in beginsel dat voor deze handeling toestemming nodig is van de rechthebbende op de software dan wel databestanden. Concreet betekent dit dat de rechthebbende op de software en/of omgeving van te voren ingelicht dient te worden over de experimenten. In de bepaling inzake onrechtmatige daad wordt rekening gehouden met de mogelijkheid – zie artikel 6:162 lid 2 BW – dat onder omstandigheden in het concrete geval sprake kan zijn van een rechtvaardigingsgrond die de daad haar onrechtmatige karakter doet verliezen. Kortom, onderzoekers kunnen een rechtvaardiging voor testen vinden in het juridisch leerstuk van de onrechtmatige daad, maar zullen in dit geval nadrukkelijk moeten kunnen aantonen welke omstandigheden de inbreuk op de rechten van derden rechtvaardigden. Deze omstandigheden zullen over het algemeen gerelateerd moeten zijn aan meer dan alleen een wetenschappelijk belang, maar ook het publiek dan wel het algemeen belang.

Met de volgende maatregelen wordt de kans op juridische problemen verkleind:

- De onderzoeker moet bij het testen van de software en eventueel binnendringen van datasystemen, zoveel als mogelijk voorkomen dat hij/zij dan wel andere leden van de onderzoeksgroep mogelijk aanwezige persoonsgegevens van derden kunnen inzien. Het beginsel van dataminimalisatie, dat wil zeggen het verwerken van zo min mogelijk persoonsgegevens als onderdeel van het uit te voeren onderzoek, dient ten alle tijden voorop te staan. Ook zal voldaan moeten zijn aan de overige zorgvuldigheidsnormen van de privacywetgeving.

- Indien in deze fase van het onderzoek serieuze kwetsbaarheden aangetroffen worden dient de 'probleemeigenaar' (typisch de producent van de software) daar zo snel mogelijk van op de hoogte te worden gebracht. Dit is de eerste stap van *responsible disclosure*. Hierbij deelt de onderzoeker eventuele kennis om de kwetsbaarheden te verhelpen. Alleen wanneer duidelijk is dat de kans groot is dat de probleemeigenaar het lopende onderzoek op onredelijke gronden direct zal willen of kunnen stilleggen, bijv. via juridische actie, is het afzien of uitstellen van *responsible disclosure* in dit stadium te rechtvaardigen.
- Om een probleemeigenaar te overtuigen van de kwetsbaarheid is vaak een overtuigend bewijs nodig. Dit bewijs dient minimaal /onschuldig / symbolisch te zijn. Het kan bijvoorbeeld bestaan uit een lijst van files die op een beschermd systeem staan (zonder de gevoelige inhoud te tonen) of een ongeautoriseerde transactie van 1 cent.

3.3.3 Verspreiding en publicatie van onderzoeksresultaten

Deze fase levert vooral mogelijke dilemma's op als het onderzoek gevoelige kwetsbaarheden (*security vulnerabilities*) aan het licht heeft gebracht. Als dit het geval is geweest moeten de acties van de betrokken onderzoekers gericht zijn op tegelijkertijd het zo snel mogelijk verhelpen van de kwetsbaarheden, en het minimaliseren van de schade. Deze twee punten zijn beide vanzelfsprekend, maar liggen niet noodzakelijk in elkaars verlengde. De snelste manier om een kwetsbaarheid te verhelpen is om die te publiceren; juist dan voelt de producent de grootste druk om het probleem op te lossen. Publicatie van een kwetsbaarheid in software vergroot echter de kans op misbruik. Bovendien is het risico aanwezig dat de producent langs juridische weg reputatie- en andere schade zal proberen te verhalen. Dit kan kansrijk zijn indien blijkt dat de onderzoeker niet de noodzakelijke zorgvuldigheid heeft betracht bij de publicatie van het onderzoek. Een vertrouwelijke melding daarentegen leidt niet altijd tot actie van de producent en kan er toe leiden dat de kwetsbaarheid langer blijft bestaan (en na verloop van tijd ook door anderen gevonden en misbruikt wordt).

Het publiceren van kwetsbaarheden is standaard praktijk op het gebied van cryptografie en computer security. Dit is onderdeel van het wetenschappelijke proces om te komen tot zo goed mogelijke beveiligingsmechanismen, waarbij sommige wetenschappers 'maken' en anderen 'kraken'. De opvatting dat het 'onder de pet houden' van kwetsbaarheden meer schade aanricht dan het publiceren ervan wordt breed geaccepteerd, ook buiten de academische wereld. Wel is het van belang dat dit op een verantwoorde wijze gebeurt, via zogenaamde *responsible disclosure*. *Responsible disclosure* kent een combinatie van:

- vroegtijdig informeren van de probleemeigenaar over de gevonden kwetsbaarheden;
- hulp aanbieden bij het verhelpen ervan;

- publiceren van de kwetsbaarheden met enige vertraging (om *zero day attacks* te voorkomen).

De probleemeigenaar dient natuurlijk geïnformeerd te worden over het voornemen tot publicatie. Discussie is er soms over de termijn die de probleemeigenaar moet krijgen om het probleem op te kunnen lossen (en er dus nog niet gepubliceerd mag worden). De *leidraad om te komen tot een praktijk van responsible disclosure* van het Ministerie van Veiligheid en Justitie noemt zestig dagen vertraging voor software, en zes maanden voor hardware. In de praktijk hoeft dit geen beperking op te leveren voor het wetenschappelijke proces. Als de onderzoekers voorafgaand aan het indienen van hun artikel bij een conferentie of tijdschrift de probleemeigenaar informeren, dan is er meestal voldoende tijd tot daadwerkelijke publicatie.

Onderdeel van het *responsible disclosure* beleid in Nederland is dat bedrijven op hun eigen website aangeven hoe meldingen gedaan kunnen worden en hoe ze afgehandeld worden. Verschillende grote bedrijven (KPN, banken) hebben hier inmiddels positieve ervaringen mee[2]. Het grootste nadeel – en risico voor onderzoekers – van *responsible disclosure* is dat de probleemeigenaar de melding niet zozeer gebruikt om de kwetsbaarheid te verhelpen, maar om de boodschapper het zwijgen op te leggen. Dit kan gebeuren door (een combinatie van) intimidatie, aansprakelijkheidsstelling, juridische actie gericht op een publicatieverbod, etc. Dit risico is reëel. In 2008 heeft het bedrijf NXP in kort geding een publicatieverbod gevraagd voor de kwetsbaarheden die onderzoekers van de Radboud Universiteit gevonden hadden in de Mifare Classic Chip van NXP. Dat verbod is door de Nederlandse rechter niet toegekend, mede op basis van vrijheid van meningsuiting. In 2013 heeft het bedrijf Volkswagen wel met succes zo'n publicatieverbod (*injunction*) verkregen van een rechter in Londen, in een zaak over kwetsbaarheden in chips in startonderbrekers. Dit verbod is twee jaar van kracht geweest en is pas na tijdrovende en langdurige onderhandelingen opgeheven. Het uiteindelijk in 2015 gepubliceerde artikel wijkt in één zin af van het oorspronkelijke artikel (zie cases in paragraaf 2.2).

Met de volgende maatregelen wordt de kans op juridische problemen verkleind:

- Bij een *responsible disclosure* dienen geen *preprints* van het artikel op het web gezet te worden. Het verdient aanbeveling (de voorzitter van) het programmacomité of de redacteur van het tijdschrift te informeren over het gevoelige karakter van het artikel, zodat de referees en anderen hierover ingelicht kunnen worden. Belangrijk is dat al deze personen zich bewust zijn van de plicht tot geheimhouding. Tegelijkertijd zullen deze partijen een vrijwaringsverklaring van de onderzoeker dan wel diens instituut verlangen. Het verdient aanbeveling hierover juridisch deskundig advies in te winnen.

2 Zie bijv. het artikel van KPN in: http://cryptome.org/2014/01/nl-cyber-sec-2013.pdf.

- De publicatie dient gericht te zijn op de wetenschappelijke aspecten van de kwetsbaarheid, zoals de ontwerpfouten, de benodigde (methodologische) verbeteringen, en de *lessons learned*. Zoveel mogelijk dient voorkomen te worden dat de publicatie een handleiding voor *hackers* wordt. Dit kan door bijvoorbeeld wel de wiskundige achtergronden te publiceren maar niet de gedetailleerde uitwerking ervan in *attack software*. Ook moet ten alle tijden voorkomen worden dat aan de hand van de resultaten de persoonsgegevens en daarmee de identiteit van individuele personen achterhaald kan worden.
- Bij onderzoek dat mogelijk juridische tegenactie van bedrijven oproept dient de leiding van de betreffende onderzoeksinstelling vooraf geïnformeerd te worden door de onderzoekers. Zulke actie kan namelijk aanzienlijke financiële risico's met zich mee brengen voor de hele instelling, en veel tijd en energie van de leiding kosten: vaak worden zowel de onderzoeksinstelling als de onderzoekers gedaagd. Omdat de onderzoekers persoonlijk gedaagd kunnen worden, als onderdeel van een intimidatiestrategie, dienen ook de bijbehorende risico's afgewogen te worden.
- Juridische risico's op een verbod tot publicatie van academisch onderzoek lijken in Nederland beperkt indien de onderzoekers nadrukkelijk de zorgvuldigheid hebben betracht die van hen naar de geldende wetenschappelijke maatstaven verlangd worden, in het algemeen belang gehandeld hebben en zorgvuldig zijn omgegaan met eventuele belangen van derden, geen illegale bronnen gebruikt hebben, geen onnodige schade berokkend hebben, en zich gehouden hebben aan de leidraad *responsible disclosure*. Indien er ook buitenlandse co-auteurs zijn betrokken kunnen eventuele rechtszaken echter ook in het buitenland worden aangespannen. Buitenlandse rechters oordelen soms anders (zie Mifarecase in hoofdstuk 2).

3.3.4 Bewaren en archiveren van zowel de gegevens als de onderzoeksresultaten

Na publicatie van de onderzoeksresultaten moeten zowel deze resultaten als het onderliggende onderzoeksmateriaal en bijbehorende correspondentie gearchiveerd en bewaard worden. Dit is van belang voor onder meer toekomstige raadpleging en verantwoording. Omdat lang niet altijd al het onderliggende onderzoeksmateriaal integraal onderdeel uitmaakt van de gepubliceerde onderzoeksresultaten, moet de onderzoeker nadrukkelijk aandacht hebben voor de archivering van dit materiaal. Zeker als het achterliggende materiaal gegevens bevat die herleidbaar zijn tot natuurlijke personen dan wel identificeerbare bedrijven (niet zijnde de rechthebbende respectievelijk de verantwoordelijken voor de onderzochte software of databestanden), dient de onderzoeker deze gegevens in geanonimiseerde vorm te archiveren. Ook zal bezien moeten worden in hoeverre archivering van achterliggend materiaal in overeenstemming is met eventueel toepasselijke eigendomsrechten op dit materiaal. Waar nodig zullen contractuele afspraken (licentie) gemaakt moeten worden. Ten slotte is het van belang dat onderzoekers beseffen dat de toepasselijke rechtsregels en ethische

overwegingen met elkaar op gespannen voet kunnen staan. Zo zal een vanuit ethische overwegingen gepropageerd *Open Access*-beleid potentieel strijdig kunnen zijn met privacybescherming. Daarom zal telkens – vanuit de specifieke context waarin het onderzoek plaatsvindt – tot een zorgvuldige weging van de verschillende belangen moeten worden gekomen.

3.4 Zorgplicht van informaticaonderzoekers

Zowel het privaatrecht, via onrechtmatige daad, als het strafrecht, onder meer via art. 450 Sr, nemen in bepaalde situaties aansprakelijkheid voor passiviteit aan. Aansprakelijkheid en daarmee sanctionering is aan de orde, zo wordt aangenomen, omdat bepaalde vormen van passiviteit in onze samenleving niet worden geaccepteerd. Het welbekende voorbeeld is de toeschouwer die aan de rand van een vijver blijft staan en nalaat een kind dat niet kan zwemmen van de verdrinkingsdood te redden. Waar precies de grenzen liggen van de juridische verplichting tot handelen, waarschuwen en hulpverlening is niet op voorhand te zeggen. Wel is duidelijk dat in situaties waarin de passieve toeschouwer een bepaalde hoedanigheid en daarmee zorgplicht ten aanzien van het slachtoffer had, eerder aansprakelijkheid wordt aangenomen. Zorgplichten zijn door te vertalen naar en daarmee ook van toepassing op de digitale omgeving. Kijkend naar diens expertise zou de specifieke hoedanigheid die een extra verantwoordelijkheid op een toeschouwer legt, wel eens van toepassing kunnen zijn op de informaticaonderzoeker. Anders gesteld, van een informaticaonderzoeker mag meer worden verwacht dan een gemiddeld internetgebruiker als het aankomt op niet passief blijven maar aan de bel trekken bij het waarnemen van opvallende zaken waar het de kwetsbaarheid van systemen aangaat. De commissie adviseert onderzoekers en onderzoeksgroepen alert te zijn op onregelmatigheid in systemen en te faciliteren dat zaken waar noodzakelijk bij handhavende instanties worden gemeld.

3.5 Conclusies

CONCLUSIE 3.1

Bij de keuze van een onderzoeksonderwerp moet het wetenschappelijke belang voorop staan en het maatschappelijke belang goed onderbouwd worden. Daarbij moet duidelijk worden gemaakt op welke wijze en in welke mate de bevindingen van het onderzoek eventuele belangen van derden kunnen raken, waaronder de privacy en intellectuele eigendomsrechten. Onderzoekers en andere betrokkenen zullen een expliciete afweging moeten maken tussen het wetenschappelijke belang en maatschappelijke belang van het onderzoek enerzijds en het belang van eventuele derden wier rechten en belangen mogelijk worden geschonden anderzijds. Het doel heiligt kortom niet altijd de middelen.

CONCLUSIE 3.2

Informaticaonderzoekers hebben een zorgplicht. Dit betekent dat passiviteit in bepaalde situaties kan leiden tot aansprakelijkheid. Onderzoekers en onderzoeksgroepen moeten daarom alert zijn en waargenomen risico's voor personen en de samenleving melden binnen de eigen organisatie en waar aan de orde aan handhavende instanties.

4. ETHICAL REVIEW BOARDS

4.1 Ethiek en Informatietechnologie

Reeds vanaf de jaren tachtig van de vorige eeuw zijn de ethische vraagstukken rond Informatietechnologie onderwerp van studie in de ethiek. Er is een vrij omvangrijke literatuur ontstaan op het gebied van de zogenaamde *Computer Ethics*[3]. Deze ontwikkeling heeft haar oorsprong in de Verenigde Staten. De beroepsorganisaties IEEE (Institute of Electrical and Electronics Engineers) en de ACM (Association for Computing Machinery), maar ook de IFIP[4,5] (International Federation for Information Processing), hebben nauwe banden met deze onderzoeksgemeenschap onderhouden wat heeft geresulteerd in een serie gedragscodes, protocollen en morele uitgangspunten voor informaticaonderzoekers en ICT-professionals. Op het gebied van *Internet Research*[6] bestaat inmiddels vrij uitvoerige literatuur. Deze literatuur is wel overwegend geïnitieerd vanuit de sociale- en gedragswetenschappen en heeft in belangrijke mate betrekking op sociale media en internet. De literatuur biedt op dit moment nog geen uitgekristalliseerde kaders voor *Ethical Review Boards* (ERB's) op het gebied van informatica.

De pragmatische benadering die voor dit rapport is gekozen is verenigbaar met de kerninzichten die in de computer ethiek zijn verworven in de laatste decennia, zoals:

3 Zie hiervoor bv. *The Cambridge Handbook of Information and Computer Ethics*, Floridi (ed.) CUP, 2010; en het artikel 'Computer Ethics' (Terry Bynum) in de *Stanford Online Encyclopedia of Philosophy*)

4 http://www.acm.org/about/se-code; https://www.ieee.org/about/ieee_code_of_conduct.pdf; https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct.

5 http://courses.cs.vt.edu/professionalism/WorldCodes/IFIP.Recommendation.html

6 Zie artikel over Internet Research Ethics in Stanford Buchanan & Zimmer http://plato.stanford.edu/entries/ethics-internet-research/

(i). computertechnologie heeft bijzondere eigenschappen die unieke morele vraagstukken met zich mee brengen (bijvoorbeeld op het gebied van de Artificial Intelligence en Autonome Systemen);
(ii). computertechnologie is een metatechnologie en derhalve alomtegenwoordig waar (smart) technologie aanwezig is;
(iii). morele waarden en keuzen van wetenschappers en ontwerpers beïnvloeden het ontwerp van ICT-diensten en -producten. Met andere woorden: ICT is niet waardenneutraal, maar is geladen met de waarden van makers, ontwerpers, onderzoekers en bedenkers;
(iv). het gaat bij het beoordelen van ICT niet alleen om computationele artefacten, algoritmen, software, IT-architecturen en IT-infrastructuren, maar om sociotechnische systemen, die zowel hardware, software, alsook de sociale (instructies, gebruiksaanwijzingen en gewoonten), juridische en institutionele aspecten omvatten. Het geheel van deze onderdelen en componenten, en het samenspel daartussen, geeft de werkelijke praktische betekenis aan ICT-diensten of -producten. Dat is buiten het ICT-domein niet anders: Een kerncentrale kan alleen veilig zijn door een combinatie van het reactorontwerp met tal van specifieke maatregelen, speciale instituties, wetten, expertise, protocollen en veiligheidscultuur. Bij de beoordeling van informaticaonderzoek moet steeds rekening worden gehouden met de manier waarop de resultaten van het onderzoek ingebed zijn of kunnen worden in een bredere sociale context.

Het voert te ver om in dit rapport een overzicht van de literatuur en van de stand van het onderzoek op dit snel groeiende gebied van de toegepaste ethiek van ICT te geven. Wij verwijzen daarvoor graag naar een aantal recente overzichtsartikelen en inleidingen [Hoven, 2010; Sullins, 2012; Zevenbergen, 2015]. Wij volstaan met een pragmatisch kader voor ethische toetsing voor informaticaonderzoek in Nederland.

4.2 Ethical Review aan kennisinstellingen

In hoofdstuk 1 is reeds verwezen naar de strengere eisen die Europese onderzoeksfondsen stellen aan de ethische kwaliteit van onderzoeksaanvragen en aan de rechtvaardiging en motivering daarvan. Het invullen van een formulier en het aankruisen van een aantal gewenste antwoorden is niet langer toereikend om goedkeuring te verkrijgen voor subsidie. Dit werpt de vraag op naar de aard van de expertise, de locus daarvan en de institutionele context van de morele evaluatiefunctie in het informaticaonderzoek in brede zin. Waar, door wie en op welke wijze zou morele toetsing van informaticaonderzoeksvoorstellen bij voorkeur plaats moeten vinden? Het antwoord op deze vraag moet rekening houden met de lessen die zijn geleerd met vergelijkbare beoordelingsinstanties en gremia in andere disciplines zoals bijvoorbeeld de geneeskunde. Bovendien moet een nieuwe instantie aansluiten bij het ecosysteem van morele

evaluatie zoals dat in de wereld van onderzoek en hoger onderwijs recent gestalte heeft gekregen. Er zijn de afgelopen jaren immers meerdere instanties bijgekomen die over ethische kwesties moeten beslissen: commissies voor arbeidsconflicten, seksuele intimidatie, gelijke behandeling, wetenschappelijke integriteit, intellectueel eigendom vraagstukken, aansprakelijkheid en *corporate governance* vraagstukken met betrekking tot deelnemingen in *start-ups*. Er is dus een vrij uitgebreide institutionele infrastructuur bij universiteiten ontstaan die betrekking heeft op uiteenlopende morele kwesties, of kwesties met belangrijke morele aspecten. Aan de orde is nu dus ook de vraag naar een instantie die naast medisch en geneeskundig onderzoek (medische ethische commissie), gedrags- en sociaal wetenschappelijke onderzoek (commissie mensexperimenten) en onderzoek dat gebruik maakt van proefdieren (de commissie dierproeven), technisch, ingenieurs-wetenschappelijk en meer in het bijzonder informaticaonderzoek moreel kan beoordelen.

4.3 Ethical Review Board Informatics (ERBI)

4.3.1 Behoefte aan een ERBI

De commissie is van mening dat het aanbeveling verdient de bestaande morele infrastructuur aan Nederlandse kennisinstellingen uit te breiden ten behoeve van de ethische beoordeling van onderzoek en onderzoeksvoorstellen van onderzoekers verbonden aan instituten of faculteiten en afdelingen waar onderzoek op het terrein van de informatica in brede zin plaats vindt. Dit soort onderzoek is zeker niet minder van invloed op mens en samenleving dan medisch, gedragswetenschappelijke en sociaal wetenschappelijk onderzoek. Informaticaonderzoek is mogelijk wijder verbreid dan en heeft tenminste evenveel impact als medisch onderzoek en kan de belangen van betrokkenen en de samenleving evenzeer raken als geneeskundig en gedragswetenschappelijk onderzoek. Het vertegenwoordigt ook een grote maatschappelijke en economische sector met alle controverses en verschillen van opvatting die daar bij horen. Ook heeft de informatica een geheel eigen en onderscheidend karakter. Dit rechtvaardigt naar de opvatting van de commissie de instelling van een eigen ethisch toetsingsinstrument. Een *Ethical Review Board Informatics* (ERBI), waar onderzoekers hun onderzoeksvoorstellen op een effectieve en efficiënte wijze ter beoordeling en toetsing voor kunnen leggen, zou moeten bestaan uit ter zake kundige en onafhankelijke informaticaonderzoekers, tenminste een jurist en een ethicus (beide met kennis en affiniteit met ICT-vraagstukken).

Sommige instellingen zijn inmiddels aan het experimenteren met een dergelijke structuur. Zo heeft de Faculteit *Electrical Engineering, Mathematics and Computer Science* van de Universiteit Twente sinds enige tijd een *Ethics Committee* en hebben de UvA, VU en CWI gezamenlijk een *Ethical Committee for Information Sciences* ingesteld. De

Universiteit Twente heeft daarnaast ook een *ethics advisor* aangesteld die onderzoekers kan helpen met het afwegen van ethische dilemma's. De Technische Universiteit Delft heeft een commissie die focust op mensexperimenten in de setting van een technische universiteit. De scope van deze commissie maakt het echter ook mogelijk dat onderzoek ter beoordeling wordt voorgelegd waarbij geen proefpersonen zijn betrokken, maar waarbij uitsluitend persoonsgegevens worden gebruikt.

Van belang is dat een ERBI goed duidelijk maakt op welke aspecten men kan adviseren zodat er geen verwarring ontstaat met het werkveld van andere commissies zoals de Medisch Ethische Commissies, de commissies rond dierproeven en de commissies rond wetenschappelijke integriteit (plagiaat, fraude, etc). Bovendien zijn er afbakeningsvragen die betrekken hebben op de verhouding tussen recht en ethiek. Juridische en ethische vragen zijn altijd lastig van elkaar te onderscheiden. Dit geldt in het bijzonder voor de informatica omdat de ontwikkelingen zeer snel gaan, vaak tot conceptuele verwarring aanleiding geven, en ons confronteren met nieuwe fenomenen. Hierdoor ontstaan er voortdurend normatief-ethische vraagstukken in een juridisch *terra incognita*. Bovendien zijn er vragen die betrekking hebben op ICT-vraagstukken waarvan te verwachten valt dat ze binnen afzienbare tijd zullen worden gereguleerd. Juridische expertise in de ERBI is dan ook van groot belang.

4.3.2 Functies en succesfactoren

De *ERB informatics* (ERBI) heeft in de visie van de commissie drie belangrijke functies:

1. Ten eerste is zij vanzelfsprekend bedoeld voor het beoordelen van informaticaonderzoek op ethische aspecten. Onderzoeksvoorstellen met duidelijke ethische aspecten gaan dan ook bij voorkeur pas van start na positieve advisering door de ERBI.
2. Ten tweede brengt zij de nodige deskundigheidsbevordering met zich mee, zodat onderzoekers en instellingen, op basis van weloverwogen oordeelsvorming, ethisch gemotiveerde verantwoording kunnen afleggen over hun informaticaonderzoek.
3. Ten slotte draagt een ERBI bij aan het morele leerproces van de organisatie en kan zij de kern en continuïteit vormen van een gemeenschap van expertise waarin kennis rond dit onderwerp wordt gedocumenteerd en al doende verder wordt ontwikkeld. Het is immers een terrein dat volop in ontwikkeling is (en zal blijven) en waar het gezamenlijke leerproces belangrijk is.

Uit de interviewronde en de klankbordbijeenkomst die de commissie heeft gehouden blijkt dat er veel draagvlak is voor dit idee. Wel bestaan er zorgen of het beoordelingsproces niet te bureaucratisch en tijdrovend gaat worden. Ook het mandaat en de

samenstelling van een ERBI waren punten van discussie. Op basis van deze geluiden uit het veld en de eerste ervaringen met een aantal ERBI's ziet de commissie een aantal succesfactoren die van belang zijn voor de goede werking van een ERBI:

i. *Nabijheid en draagvlak binnen community*. De ERBI's kunnen alleen goed functioneren als de afstand tussen ERBI's en onderzoekers zowel fysiek als mentaal niet te groot is. Als een of enkele leden van de ERBI afkomstig zijn uit de eigen eenheid maakt dit de drempel om vroegtijdig advies te vragen lager. Om het draagvlak te vergroten moeten leden van de ERBI door collega-onderzoekers als gezaghebbend worden gezien. De ERBI zal dan ook sneller worden gezien als een herkenbare entiteit. Bovendien maakt lokale nabijheid het praktisch eenvoudiger om als ERBI frequent bijeen te komen. De voorkeur gaat daarom uit naar lokale ERBI's (op het niveau van een faculteit, onderzoeksinstituut, of universiteit) boven bijvoorbeeld een landelijke ERBI voor al het informaticaonderzoek. De nabijheid kan uiteraard ook een keerzijde hebben in de vorm van al te grote bekendheid tussen aanvrager en beoordelaar. Voor belangenverstrengeling door te nauwe collegiale relaties tussen beoordelaars en indieners moet worden gewaakt. Gangbare regels voor het melden van (potentiële) *conflicts of interest* bij het *reviewen* en beoordelen van artikelen, manuscripten en onderzoeksaanvragen zijn ook hier van toepassing.
ii *Snelheid*. Ook de frequentie van vergaderingen en de snelheid van afhandeling van aanvragen is belangrijk voor een goed functioneren en voor het vertrouwen dat wetenschappers in de ERBI zullen hebben. Onderzoekers staan vaak onder grote tijdsdruk en zien zich geconfronteerd met onverbiddelijke en belangrijke deadlines. Om de efficiëntie bij een groot aantal onderzoeksvoorstellen goed te kunnen managen stellen wij in hoofdstuk 5 een selectie- en beoordelingsprocedure voor.
iii. *Status van het advies*. De normatieve status en legitimiteit van het advies zijn belangrijk. Ondanks dat onderzoekers altijd zelf geacht worden een morele afweging te maken, en zij hun morele verantwoordelijkheid nimmer kunnen overdragen, moeten zij zich kunnen verlaten op het oordeel van de commissie. Anderzijds moeten de leden van ERBI's ook gevrijwaard worden door de universiteit tegen aansprakelijkheidsclaims. De ERBI moet worden ingesteld door het bestuur of directie van de betreffende onderzoekseenheid. De ERBI adviseert ook in formele zin aan directie of bestuur om onderzoek al dan niet uit te voeren. De operationele verantwoordelijkheid voor wat er met de adviezen wordt gedaan ligt niet bij de ERBI maar bij het bestuur. De commissie onderhoudt een ordentelijk archief, inclusief notulen van haar vergaderingen en legt verantwoording af bij (voorkeur jaarlijks) aan bestuur of directie.
iv. *Scope en afbakening*. Een ERBI moet goed duidelijk maken waarvoor men wel en niet bestemd is. Hiertoe moet een aantal vragen worden beantwoord. De eerste vraag betreft de disciplinaire achtergrond van de aanvragers. Niet alleen aanvragen uit informaticafaculteiten zouden bij deze ERBI ingediend moeten kunnen

worden, maar ook aanvragen uit andere faculteiten die informaticaonderzoek doen. Aan technische universiteiten vindt bijvoorbeeld ook informaticaonderzoek plaats bij faculteiten als werktuigbouwkunde (robotica en *high tech systems*), civiele techniek, lucht- en ruimtevaarttechniek, technische bestuurs- en bedrijfskunde.

v. *Omvang en locus*. Omdat niet alle faculteiten groot genoeg zijn om voldoende voorstellen te genereren kunnen faculteiten eventueel besluiten om samen te werken of gezamenlijk een ERBI informatica in te stellen. Wel is het van belang dat deze lokale commissies onderling afstemmen en van elkaar leren. Een netwerk van ERBI's moet idealiter gaan functioneren als een lerende organisatie. Een analogie kan hier worden getrokken met de Commissies Wetenschappelijke Integriteit (CWI). In enkele jaren tijd hebben alle universiteiten een dergelijke commissie in het leven geroepen. De KNAW heeft samen met NWO en VSNU een Landelijk Orgaan Wetenschappelijke Integriteit gevestigd, waarbij klagers in beroep kunnen gaan tegen beslissingen in hun zaak door het College van Bestuur van hun universiteit. Ook bestaat er inmiddels een landelijk overleg van voorzitters van CWI's die ervaringen, *best practices* en geanonimiseerde 'moresprudentie' uitwisselen. Ook zijn zij voornemens de VSNU aanbevelingen te doen over aanvulling op de landelijke code wetenschappelijke integriteit. Institutionalisering op het gebied van ERBI's biedt op zich een vergelijkbaar proces. De commissie pleit ervoor dat niet iedere ERBI dit zelfstandig doet, maar gaat samenwerken met andere ERBI's. Zij kunnen met elkaar aan intervisie doen door bijvoorbeeld de normenkaders op elkaar af te stemmen en casuïstiek, ideeën en ervaringen uit te wisselen. In de kring van SURFnet is bijvoorbeeld ervaring opgedaan met een dergelijke structuur. SURFnet heeft een community opgezet van leden van de zogenaamde CSIRTs (*Computer Security Incident Response Teams*) van aangesloten instellingen. Deze community wil synergie bereiken onder beveiligingsexperts en organiseert daarvoor onder andere bijeenkomsten en trainingen. De leden van de community bepalen zelf de agenda van de bijeenkomsten. Ook heeft de community zelf een lidmaatschaps- en gedragscode opgesteld.

Gedistribueerde onderzoeksprojecten

Onderzoeksprojecten worden steeds vaker in samenwerking met andere instellingen uitgevoerd. Dit stelt ook eisen aan de manier waarop ERBI's worden georganiseerd en hoe tot onderlinge afstemming kan worden gekomen. Een belangrijk aandachtspunt voor het opzetten van een goed functionerend ERBI-netwerk wordt gesignaleerd en geanalyseerd in het artikel [Dove, 2016]. In dit artikel wordt gekeken naar de ethische aspecten van *multi-site research*, onderzoek dat gedistribueerd is over verschillende instellingen, locaties, of zelfs landen. Dit komt vooral voor bij internationaal onderzoek

met een sterk data-georiënteerd karakter. Op dat gebied is er nog geen *top-down*-internationale regulering, reden waarom hier en daar *bottom-up*-benaderingen zijn ontwikkeld.

Het artikel schetst drie principes en bijbehorende modellen om bij *multi-site* onderzoek, waarbij dus meerdere ERBI's betrokken kunnen zijn, tot onderlinge afstemming te komen. Het model 'reciprociteit' is gebaseerd op het principe dat de leden in een ERBI-netwerk wederzijds elkaars beslissingen erkennen. Voordelen van dit model zijn dat het proces flexibel kan blijven en dat de lokale autonomie behouden kan blijven. Nadelen zijn het 'gevaar' van inconsistente of incompatibele oordelen; onduidelijkheid over de kwaliteitsverschillen tussen de oordelen van de verschillende leden en een lastig implementatieproces in de opstartfase.

Het model 'delegeren' is gebaseerd op het principe dat de leden van het netwerk in onderlinge overeenstemming besluiten welk lid of leden het betreffende onderzoek beoordelen. De voordelen van dit model zijn dat er minder kans is op inconsistente beoordelingen en dat er een taakverdeling gebaseerd op lokale expertise mogelijk is. De nadelen zijn dat het lastig is om zo'n delegering te kiezen, de nazorg van beoordelingen minder eenvoudig is en dat er weinig ruimte is voor alternatieve oordelen.

Het model 'federatie' heeft als kernprincipe dat er een centrale ERBI wordt gecreëerd waarin representanten van de verschillende ERBI-leden zitting hebben. Als voordelen worden genoemd dat het kosten effectief is omdat dubbel werk wordt voorkomen, het aantal inconsistente reviews wordt gereduceerd en dat het bijdraagt aan de opbouw van een groepscultuur voor reviews. Als nadelen worden gesignaleerd dat het lastig is om met lokale en culturele verschillen om te gaan, dat er verschillende machtsverhoudingen kunnen zijn binnen zo'n federatie en dat het moeilijk kan zijn om onderlinge overeenstemming te bereiken.

Belangrijke conclusie van het artikel is dat er op dit moment nog geen efficiënt en bevredigend systeem is voor de beoordeling van data-intensief *multi-site*-onderzoek. De onderzoekers doen daarom de aanbeveling om het voorlopig maar op een ad-hoc- en bottom-up-manier te doen. Idealiter gebeurt dit met instemming van de betrokken financiers. Naarmate de diverse modellen meer getest worden en ontwikkeld, kunnen meer 'systemische' oplossingen geïmplementeerd worden. Hiertoe dienen bruikbare metrieken te worden ontwikkeld om kwaliteit en efficiency van ERBI-netwerken te evalueren. Deze observatie sterkt de commissie in haar mening dat we in Nederland moeten streven naar een netwerk van lokale ERBI's die gezamenlijk een normenkader gaan ontwikkelen.

4.4 Richtinggevend praktisch kader voor ethische afweging

Er is geen blauwdruk of ideaalbeschrijving voor een ERBI en er is ook geen vastgesteld ethisch normenkader voor haar werkzaamheden. Bovendien is te verwachten dat de omgeving waarin de ERBI's moeten werken continu aan technische, wetenschappelijke, morele en juridische verandering onderhevig is. De informaticavraagstukken van nu zijn deels anders dan die van een jaar geleden en die van volgend jaar zijn nog niet alle te voorzien. Een ERBI moet dus voor zichzelf een werkwijze en een normenkader ontwikkelen dat (a) het relevante recht en jurisprudentie accommodeert en (b) voldoet aan *best practices* in de toegepaste ethiek van ICT en (c) conform is aan de *state of the art* in het denken over ERBI's in het algemeen. De ERBI moet er ook voor zorgen dat haar overwegingen steeds weer aansluiten bij nieuwe ontwikkelingen in ICT en het informaticavakgebied. De leden van een ERBI zullen zichzelf daarin ook moeten blijven ontwikkelen.

Wij schetsen in hoofdstuk 5 een algemeen kader aan de hand waarvan ERBI's hun werk kunnen ondersteunen en structureren. We bieden een schets van hoe een triage model in dit verband zou kunnen werken, mede gebaseerd op beperkte ervaringen die hiermee zijn opgedaan. Wij geven voorts de contouren van een moreel afwegingskader dat niet bedoeld is als ethische checklist, maar als een manier om mogelijk relevante morele overwegingen te articuleren wanneer leden van ERBI's hun discussies over de morele aanvaardbaarheid van onderzoeksvoorstellen voeren. Ten slotte geven wij in hoofdstuk 5 een aantal aandachtspunten en een aantal vragenlijsten die belangrijke aspecten van ICT-onderzoek adresseren. Tezamen vormen zij een handreiking die enig houvast kan bieden voor informatica-onderzoekers en leden van ERBI's.

4.5 Conclusies en aanbevelingen

CONCLUSIE 4.1

Het instellen van een *Ethical Review Board Informatics* en het monitoren van haar prestaties en de reflectie op de aldus verworven inzichten, is een van de manieren waarop de informaticaonderzoeksgemeenschap gestalte kan geven aan haar morele en maatschappelijke verantwoordelijkheid alsmede uitdrukking kan geven aan het besef dat informatica een belangrijke vormgever is van de samenleving.

AANBEVELING 4.1

De commissie raadt alle besturen van instituten of afdelingen actief op het terrein van informaticaonderzoek aan om, al dan niet samen met collega-instellingen, een *Ethical Review Board Informatics* (ERBI) in te stellen. Deze ERBI's hebben als primaire taak het beoordelen van informaticaonderzoek op ethische aspecten. Daarnaast kan een ERBI fungeren als de kern van een gemeenschap waarin kennis rond dit onderwerp verder kan worden ontwikkeld.

AANBEVELING 4.2

De ethische toetsing van informaticaonderzoek staat nog in de kinderschoenen. Er is dan ook geen blauwdruk of ideaalbeschrijving voor een Ethical Review Board Informatics te geven en er bestaat ook geen vastgesteld normenkader. Bovendien is informatica een bijzonder dynamisch vakgebied waardoor de informaticavraagstukken van volgend jaar nu nog niet te voorzien zijn. De ERBI's wordt aangeraden voor zichzelf een werkwijze en een normenkader te ontwikkelen en dat te doen in nauw overleg met andere ERBI's.

5. AANZET VOOR EEN BEOORDELINGSPROCEDURE

5.1 Inleiding

De afgelopen decennia is er een grote ontwikkeling geweest in 'computer ethiek', of de 'ethiek van ICT'. Dit zal in de komende tijd nog versterkt worden door de toenemende opkomst en invloed van tal van emergente technologieën zoals *cybersecurity*, *drones*, *big data*, *artificial intelligence*, robots, sensoren en *quantum computing*, om een verre van uitputtende opsomming te geven. Niet alleen in deze specifieke gebieden, maar in informaticaonderzoek in het algemeen zullen steeds vaker hoge morele standaarden worden aangelegd. Dit komt al tot uiting in de eisen die gesteld worden door onderzoeksorganisaties en hun beoordelingsprocedures. Voor publicaties, beurzen en projectverwerving is vaak goedkeuring vereist van een ethische toetsingscommissie of procedure.

5.2 Morele waarden

Ethische overwegingen kunnen betrekking hebben op belangen, noden, voorkeuren, rechten, plichten, verantwoordelijkheid en karakterdeugden. Ze kunnen aandacht vragen voor de gevolgen voor mensen in termen van gezondheid, geluk of geldelijk gewin en ze kunnen de nadruk leggen op de intenties van personen. Zoals we bij de juridische aspecten de principes hanteren die vastgelegd zijn in *wetten*, hebben we bij de ethische aspecten als arsenaal van principes de ethische, morele *waarden*. Morele waarden zijn algemeen gangbare aanduidingen van morele soorten van overwegingen zoals: 'respect', 'privacy', 'geluk', 'waardigheid', 'veiligheid' en 'duurzaamheid'. Overal

waar mensen ethische afwegingen maken worden morele waardetypen gebruikt om morele overwegingen te articuleren. Er zijn echter zeer veel verschillende en uiteenlopende waarden die niet tot elkaar gereduceerd kunnen worden: het zogenaamde waardenpluralisme, dat we in de volgende paragraaf nader toelichten. De morele waarden vormen tezamen een afspiegeling van de morele complexiteit die ons leven en ons soort samenlevingen karakteriseert. Onze morele systemen en de ethische reflectie daarop is navenant complex en divers.

De consequenties van de complexiteit van het waardendomein

De complexiteit en diversiteit van het waardendomein heeft gevolgen voor de ethische beoordeling van informaticaonderzoek. Het is goed om ons hier expliciet rekenschap van te geven. De Engelse filosoof Isaiah Berlin verwoordt dit als volgt: Het universum van *ethische waarden* heeft een zeer gecompliceerde structuur. Waarden kunnen niet geordend worden langs een lineaire schaal die zegt dat van twee waarden de een belangrijker is, meer waardevol, dan de ander. Ze zijn niet *commensurate*, onderling meetbaar. Ook kunnen waarden met elkaar in conflict zijn, een stel waarden kan *inconsistent* zijn. Dit inzicht staat bekend als waardenpluralisme (*value pluralism)* en heeft voor het werk van ERBI's een aantal belangrijke gevolgen. Een eerste gevolg is dat in sommige situaties gekozen moet worden tussen de waarden die men wil handhaven of bevorderen. Een ander gevolg is dat er geen *a-priori*-vastomlijnd kader kan zijn voor de ethische beoordeling. Situaties kunnen niet eenduidig geclassificeerd of gepositioneerd worden in de ruimte van waarden. Dit betekent ook dat het niet mogelijk is om voor een ERBI een vastomlijnd beoordelingskader te maken. Dit maakt dat de commissie in dit rapport ook geen 'handleiding' voor de beoordeling van onderzoek in een ERBI kan geven. Wat we wel hebben geprobeerd is het formuleren van een *handreiking*, en een gedifferentieerde beoordelingsprocedure. Deze zal zich gaandeweg moeten ontwikkelen, gevoed door voortschrijdend inzicht, ervaringen en toenemende 'moresprudentie'.

Een vraag die bij bovenstaande observatie rijst, is waarom er in de medische hoek met zijn METC's kennelijk wel een goed werkend ethisch beoordelingskader is. Onze indruk is dat een mogelijk verschil tussen de situatie van medisch onderzoek versus informaticaonderzoek ligt in het aspect van de breedte van de problematiek, die maakt dat de pluraliteit het wint van de systematiek. Meer concreet: het toetsingskader voor METC's is per wet zeer smal, namelijk uitsluitend met aandacht voor *gevaar voor proefpersonen*. Dit geeft zo'n smal kader dat criteria en toetsing beduidend eenvoudiger worden.

Morele waarden in informaticaonderzoek

Een zeker niet uitputtend overzicht van morele waarden die van toepassing zijn bij informaticaonderzoek is weergegeven in tabel 5.1. Ondanks de voorgaande signalering dat er geen eenduidige classificering of structuur in het waardendomein mogelijk is, heeft de commissie geprobeerd enige structuur aan te brengen door de veel voorkomende waarden in informaticaonderzoek te verdelen over drie kolommen (tabel 5.1). De linker kolom bevat waarden die primair als predicaat aan één individu worden toegeschreven (Jan is veilig, Jan is gezond, happy, …). De middelste kolom bevat waarden die primair van toepassing zijn op een relatie tussen twee individuen. De derde kolom bevat waarden die vooral naar een morele kwaliteit van een omvattend sociaal systeem verwijzen.

Tabel 5.1 Morele waarden die bij informaticaonderzoek voorkomen

primair van toepassing op één individu	primair van toepassing op een relatie tussen twee individuen	primair van toepassing op een sociaal systeem
health	responsibility	respect
wellbeing	accountability	dignity
physical integrity	justice	non-discrimination
happiness	equity	transparency
privacy	solidarity	trust
security	autonomy	democracy
safety	confidentiality	freedom
knowledge	access	utility

Belangen van anderen: stakeholders (direct en indirect) en 'affected persons'

Ethiek heeft primair betrekking op rekening houden met de belangen, rechten, noden van anderen, en met de beperkingen die daaruit voortvloeien voor het behartigen van het eigenbelang. Door een adequate conceptualisering wordt er zorg voor gedragen dat 'anderen' worden gerepresenteerd in de morele afweging, ook al zitten zij niet aan tafel, of kunnen zij om wat voor reden dan ook niet voor zichzelf spreken. Hierdoor kan toch hun veiligheid, welzijn, en geluk, vrijheid en privacy meewegen in de besluitvorming. Het kan dan gaan om gebruikers van een technologie over enkele jaren, of om de personen die de effecten van het gebruik zullen ervaren op de een of ander manier enkele jaren na de introductie van desbetreffende technologie. In de ethiek is reeds veel ervaring opgedaan met het ethisch beoordelen van technologie in bijvoorbeeld: Maatschappelijke Kosten Baten Analyses (MKBA's), *Technology Assessment (TA),* en *Privacy Impact Assessments (PIA)*, *Data Protection Assessment*, *Ethical and Legal and Social Aspects (ELSA)* en recent Maatschappelijk Verantwoord Innoveren (MVI) of in

EU context *Responsible Research and Innovation (RRI)*. In deze benaderingen van de ethiek van techniek is een belangrijk deel van de aandacht gewijd aan het identificeren en conceptualiseren van moreel relevante personen en groepen in verband met de morele beoordeling van techniek.

5.3 Een internationale rondgang

Als input bij het opstellen van een beoordelingsprocedure – die als startpunt kan dienen voor de in hoofdstuk 4 bepleite ERBI's – zijn ethische protocollen en richtsnoeren van binnen- en buitenlandse organisaties verzameld en geanalyseerd (zie bijlage 3). Hieruit komt een aantal algemene observaties naar voren:

- *Beperking in scope:* De meerderheid van de beschikbare protocollen en richtlijnen heeft alleen betrekking op de ethische aspecten van de *identificeerbare onderzoekssubjecten*. Dit is bijvoorbeeld het geval bij proefpersonen in medische experimenten of in biometrische experimenten, *serious games* en *video taped sessions*, vragenlijsten etc. Ethische aspecten van de effecten van het onderzoek op de *maatschappij of milieu* worden bijvoorbeeld zelden meegenomen. Ook werd er in de door ons geïdentificeerde literatuur weinig aandacht geschonken aan nationale veiligheid, en aan *dual-use*-kwesties.
- *Gemeenschappelijke kern:* Vrijwel alle gevonden onderzoeksprotocollen en ethische richtlijnen zijn redelijk eenduidig over het belang van onderwerpen als *informed consent*, *invasive interventions*, *participation of minors*, kwetsbare groepen. In vrijwel alle protocollen wordt hier aandacht aan besteed.
- *Proportionaliteitsbeginsel:* Veel protocollen en richtlijnen gaan uit van het proportionaliteitsbeginsel: de verplichtingen rond *accountability*, *documentation*, *reporting* en *monitoring* zijn afhankelijk van het risico en scope van het onderzoek en het type experimenten dat wordt uitgevoerd. Een uitgebreid *Research Data Management Plan* en *Privacy Impact Assessments* (PIA's) zijn bijvoorbeeld alleen noodzakelijk voor onderzoeken met aanzienlijke impact voor grote groepen deelnemers.
- *Verantwoordelijkheid voor studenten:* Veel protocollen benadrukken dat als het onderzoek door studenten wordt uitgevoerd de verantwoordelijkheid voor de ethische goedkeuring bij een lid van de wetenschappelijke staf moet liggen.

Het is duidelijk dat de internationale inventarisatie bevestigt dat er geen pasklaar generiek ethisch beoordelingskader te maken is. Ook al geeft het een houvast de gemeenschappelijke kern uit de internationale richtlijndocumenten te constateren, we hebben ook geconstateerd dat er een aanzienlijke beperking in scope is, waardoor tal van problematische kwesties niet bestreken worden. Dit maakt een gezamenlijke ontwikkeling van het beoordelingskader door de ERBI's noodzakelijk.

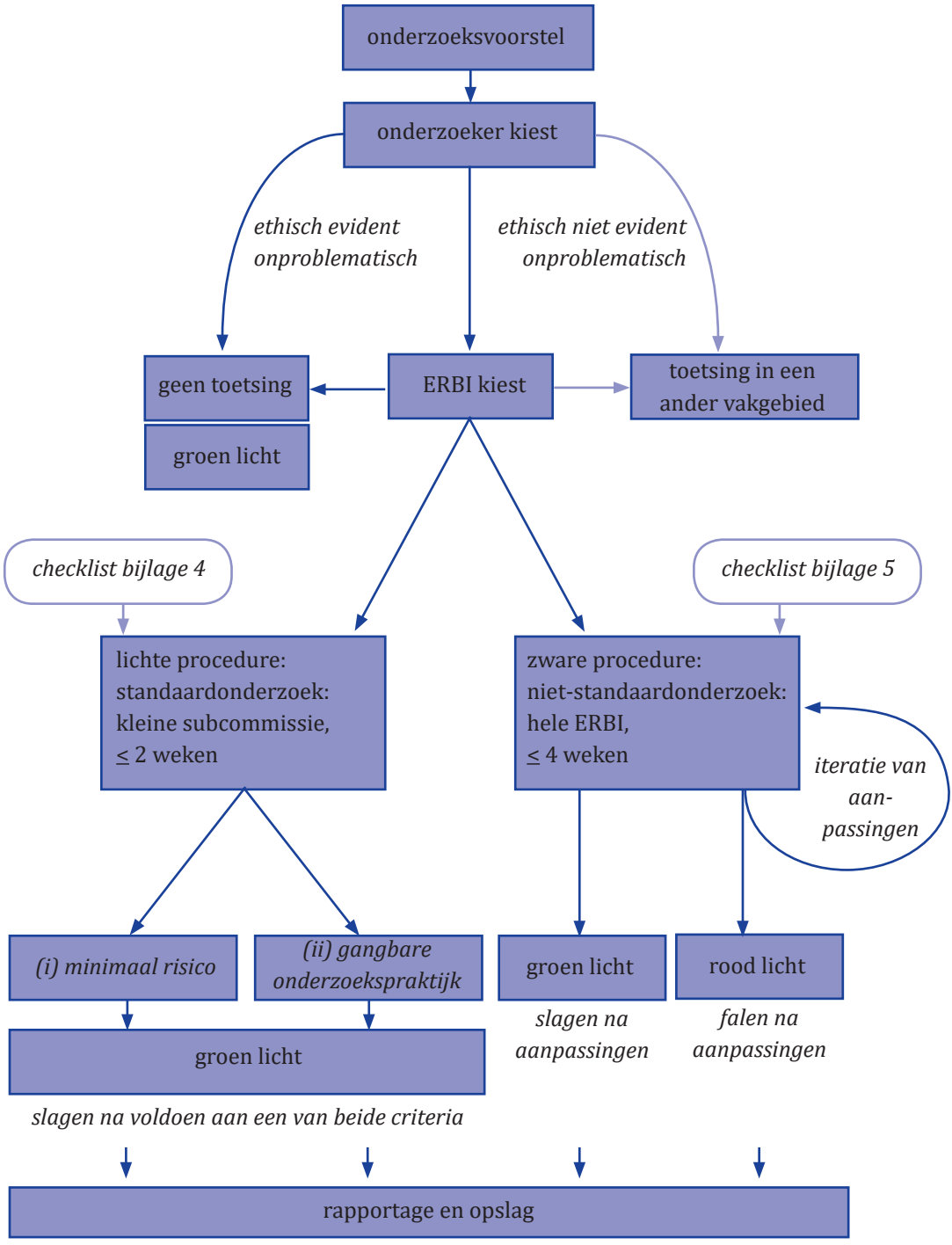
5.4 De ERBI aan het werk: voorstel voor een werkwijze

Wetenschappers worden geacht om grondig na te denken over morele waarden in relatie tot hun onderzoek en de risico's die het direct of indirect met zich mee kan brengen voor alle directe en indirecte stakeholders en '*affected persons*'. Het overzicht van morele waarden in tabel 5.1 kan hierbij als startpunt dienen. Een ERBI wordt gevraagd zich een oordeel te vormen over de wijze waarop het voorgestelde onderzoek, zowel wat doelstelling, (on)bedoelde, (on)voorziene resultaten en effecten betreft, als ook voor wat betreft de gevolgde procedures, methodes en werkwijze, een positief of negatief verschil kan maken voor alle mogelijke betrokkenen, nu en in de toekomst. Dus zowel vragen naar de privacy en veiligheid van personen van wie de data worden gebruikt alsook vragen naar de effecten op sociale uitsluiting of discriminatie op de lange termijn zijn nadrukkelijk aan de orde. In deze paragraaf wordt een procedure voorgesteld die ERBI's kunnen gebruiken voor een efficiënte werkwijze (zie ook figuur 5.1). Deze procedure is gebaseerd op het principe van triage, het zo snel mogelijk verdelen van de voorstellen in verschillende categorieën gebaseerd op de complexiteit van de ethische afweging.

Rol van de onderzoeker

Bij een aantal in te dienen onderzoeksvoorstellen kan de onderzoeker zelf op basis van gezond verstand al wat *a-priori*-voorwerk doen om een overbodige stap in het proces van beoordeling te vermijden. Voor veel puur theoretisch onderzoek is het bijvoorbeeld evident dat het ethisch neutraal is en geen toetsing nodig is. Wanneer de onderzoeker meent dat het onderzoek ethisch niet evident neutraal is, moet het voorstel aan een ERBI worden voorgelegd. Bekendheid met de cases zoals beschreven in paragraaf 2.2 of meer algemeen een ethisch/juridisch bewustzijn van mogelijk risico's, dilemma's en gevaren, zal een onderzoeker helpen om deze beslissing te nemen. Deze beslissingen zullen ook gemakkelijker gemaakt kunnen worden als in het betreffende onderzoeksveld het algemene bewustzijn rond dit onderwerp actief wordt bevorderd. In het volgende hoofdstuk worden hiertoe aanbevelingen gedaan.

Bij sommige typen onderzoek moet het onderzoeksvoorstel door een commissie uit een ander vakgebied worden getoetst. Dit is bijvoorbeeld het geval bij bepaalde typen medisch-wetenschappelijk onderzoek dat verplicht aan een METC moet worden voorgelegd (zie paragraaf 2.3). Indien de onderzoeker hierover twijfelt, kan hij/zij de ERBI om advies vragen. Idealiter zal hier een samenspel ontstaan tussen onderzoeker en ERBI, waarbij we opmerken dat de grens van de verantwoordelijkheid tussen individuele onderzoeker en ERBI voor deze beginstap van de procedure op dit moment nog niet scherp is af te bakenen.



Figuur 5.1 Voorstel beoordelingsprocedure

Start van de procedure: de intake beoordeling

Bij alle voorstellen die bij een ERBI worden ingediend controleert de secretaris of de betreffende onderzoeker juist heeft gehandeld door dit bij een ERBI en niet bij een andere instantie in te dienen. Wanneer dit is geverifieerd volgt de volgende beoordelingsstap.

Toetsing: kan worden volstaan met lichte procedure?

In deze beoordelingsstap wordt bepaald of het voorstel in aanmerking komt voor een lichte procedure. Dit is het geval voor onderzoek dat kan worden gezien als min of meer 'standaardonderzoek'. Hiervoor kan gebruik worden gemaakt van vragenlijsten waarvan een voorbeeld is gegeven in bijlage 4. Met behulp daarvan wordt getoetst op twee (grotendeels) los van elkaar staande criteria:

1. Beoordeling van *minimaal risico*; bij een minimaal risico beoordeling wordt de vragenlijst gebruikt om vast te stellen of het onderzoek meer dan slechts minimaal risico met zich meebrengt. Minimaal risico wordt hierbij vaak gedefinieerd als het risico niveau dat gebruikelijk is in het alledaagse leven.
2. Beoordeling van *gangbare onderzoekspraktijk*; deze beoordeling bepaalt of het voorgestelde onderzoek voldoet aan criteria voor standaard onderzoek. Zulke criteria verschillen veelal per (sub)discipline; de ontwikkeling van lijsten van criteria per (sub)discipline is een taak van de ERBI bij de start van haar bestaan. Dit moet gebeuren in een evoluerend proces en met onderlinge uitwisseling tussen de diverse ERBI's.

Onderzoek dat voor een van beide toetsen slaagt kan worden beoordeeld volgens een lichte procedure, bijvoorbeeld alleen door de secretaris en voorzitter van de ERBI (of, in het geval er verschillende afdelingen betrokken zijn, door een relevant lid van de ERBI). Deze procedure neemt meestal niet meer dan 2 weken in beslag, bij onderzoekseenheden die met dit scenario werken. Voorbeelden van dergelijke procedures zijn weergegeven in kader 5.1.

KADER 5.1 VOORBEELDPROCEDURES

Een voorbeeld van een faculteit die een onderscheid maakt in een lichte en een zware procedure is de *Faculty of Electrical Engineering, Mathematics and Computer Science* van de Universiteit Twente die in het *protocol for assessing the ethical permissibility of proposed research* bijvoorbeeld het concept *standard research* heeft geïntroduceerd. Veel onderzoek dat in een faculteit wordt uitgevoerd is niet compleet nieuw. Vanuit methodologisch en ethisch perspectief is een deel van het onderzoek slechts een geringe aanpassing van eerder verricht onderzoek. Men onderscheidt daarom standaard en niet-standaard onderzoek. Standaard onderzoek is onderzoek dat men in het verleden op min of meer

reguliere basis heeft uitgevoerd. Dit onderzoek mag via de lichte procedure worden geaccordeerd. Voor alle onderzoeksgroepen is gedefinieerd wat voor onderzoek als standaard kan worden gezien. Vergelijkbare procedures zijn bijvoorbeeld ook te vinden bij de *School of Computer Science and Statistics* van de universiteit van Dublin en de TU Delft. Aan de TU Delft komen alle aanvragen bij de voorzitter binnen en die maakt een eerste schifting tussen gevallen die moeten worden besproken en gevallen, waarin naar het oordeel van de voorzitter geen enkel bespreekwaardig moreel probleem aan de orde is. Er wordt een lijst bijgehouden van alle binnengekomen aanvragen en deze wordt gedeeld met alle leden van de commissie. Het staat de leden van de commissie vrij de beslissing van de voorzitter te agenderen en om herziening van dit oordeel te verzoeken.

Zwaardere procedure

Indien het voorgestelde onderzoek niet voldoet aan een van de twee criteria uit de vorige stap is een grondigere afweging en/of meer informatie noodzakelijk. Over dit type onderzoek moet de gehele ERBI zich buigen waarbij eventueel in overleg met de betreffende onderzoekers het voorstel kan worden aangepast. Deze procedure neemt naar verwachting niet meer dan een maand in beslag.

Als verdere handreiking heeft de commissie uit de internationale vragenlijsten en onze eigen analyse een aantal vragen gedestilleerd die kunnen helpen bij de verdere afweging. Deze zijn gegroepeerd rondom vier onderwerpen, vragen over:

a. het doel van het onderzoek
b. de resultaten en opbrengsten
c. de onderzoeksmethode en aanpak
d. *affected persons* en *stakeholders*

(a) Doel van het onderzoek

- Is aannemelijk te maken dat het doel van het onderzoek onverenigbaar is met bestaande of toekomstige wetgeving of morele waarden en morele idealen, *human rights and standards of public conscience*, en menselijke waardigheid?
- Is het doel van het onderzoek gericht op uitkomsten die kunnen leiden tot het verslechteren van morele waarden zoals gezondheid, welzijn, autonomie, veiligheid, geborgenheid, privacy, vertrouwelijkheid, verantwoordelijkheid, transparantie, accountability, aansprakelijkheid, rechtvaardigheid, ongelijkheid, sociale rechtvaardigheid, menselijke waardigheid?
- Is het doel van het onderzoek op enigerlei wijze in positieve zin gericht op het menselijk gezondheid, welzijn en geluk?
- Hoe kan dit onderzoek (mits het niet puur fundamenteel onderzoek betreft ten

bate komen van de maatschappij, welke bijdrage mag worden verwacht aan het oplossen van maatschappelijk problemen of de grote maatschappelijke uitdagingen?

(b) Resultaten en opbrengsten

- *Risico op dual use:* Kunnen de resultaten, artefacten of systemen voortkomend uit dit onderzoek: direct of indirect worden gebruikt voor de vervaardiging van wapens?
- *Risico op misuse:* Kunnen de resultaten van het onderzoek:
  - potentieel gebruikt worden voor criminele, terroristische of anderszins illegale activiteiten?
  - op een of andere manier schadelijk zijn voor gebruikers, of gebruikt worden voor discriminatie of onderdrukking van mensen?
  - gebruikt worden om het lastiger of onmogelijk te maken voor bepaalde betrokken partijen om hun verantwoordelijkheid te nemen, of kan het bijdragen om wettelijke of morele overtredingen van gebruikers meer waarschijnlijk te maken?
  - een negatieve invloed hebben op het milieu, veiligheid of gezondheid?

(c) Onderzoeksmethode en aanpak

In de geanalyseerde vragenlijsten en protocollen gaan veruit de meeste vragen over de onderzoeksmethode en -aanpak. Een voorbeeld van een uitvoerige checklist over dit aspect is opgenomen in bijlage 5.

(d) Affected persons en stakeholders

- Zijn de belangen van alle relevante stakeholders en *affected parties* in ogenschouw genomen?
- Zijn er groepen of partijen in de samenleving die zeer tegen dit onderzoek gekant zouden zijn, en zo ja waarom?
- Op wie kan het onderzoek en de resultaten ervan impact hebben?
- Kan het onderzoek effecten hebben die pas op langere tijd zichtbaar worden?
- Zijn er bijzonder kwetsbare groepen die benadeeld kunnen worden door het onderzoek?
- Hoe zou de samenleving veranderen als het onderzoek en de resultaten ervan zeer grote impact zouden hebben en overal ingang zouden vinden?

5.5 Rapportage en opslag

Na de procedure in de ERBI moet het vastgestelde advies worden gecommuniceerd en vastgelegd. Het is denkbaar dat er geen unaniem advies kon worden bereikt. In dat geval is het zinvol om minderheidsposities te documenteren opdat naderhand kan worden achterhaald op welke gronden de kritiek van deze minderheid toch niet als doorslaggevend is bevonden. Hierbij is van belang dat het in de rapportage bevatte advies is gebaseerd op een adequate, maar niet noodzakelijk tot eenduidige conclusies leidende, afweging van de verschillende belangen en waarden.

De rapportage over een onderzoeksvoorstel gaat uiteraard naar de onderzoeker(s) en ook naar het management van de betreffende onderzoeksorganisatie. Daarbij wordt van de onderzoeker verwacht dat deze zich conformeert aan de uiteindelijke en mede na hoor en wederhoor en eventuele aanpassing van het voorstel tot stand gekomen aanbeveling van de ERBI. Dit is primair relevant wanneer de ERBI negatief adviseert inzake de uitvoering van het onderzoek. De taak om er op toe te zien dat het onderzoek in die vorm niet wordt uitgevoerd, ligt echter bij het management van de onderzoeksorganisatie, en niet bij de ERBI.

Zoals eerder aangegeven moet het beoordelingskader nog groeien. Daarom is het van groot belang dat ERBI's hun verslagen vastleggen op een manier dat die toegankelijk is voor onderzoekers maar zeker ook voor andere ERBI's. Het verdient aanbeveling dat de ERBI's op termijn werken aan een gezamenlijke manier van ontsluiten waarin alle beslissingen te raadplegen zijn. Deze ontsluiting van 'moresprudentie' biedt de mogelijkheid tot het checken van consistentie, convergentie van beoordelingen.

In zeer uitzonderlijke gevallen is het mogelijk dat de ERBI dringend aanbeveelt het onderzoek in elk geval wel uit te voeren omdat daarmee grote belangen van derden gemoeid zouden zijn. We geven twee recente voorbeelden om de gedachten te bepalen. Een voorbeeld, met dramatische gevolgen op korte termijn, is het onderzoek naar het ZIKA-virus. Allerlei detectietechnieken, *computer vision* technieken etc. kunnen heel goed in het kader van huidig en toekomstig informatica- en ICT-onderzoek vallen. Een ander recent voorbeeld, met dramatische gevolgen op de lange termijn, is de recente oproep van de Verenigde Naties naar intensief en grootschalig onderzoek naar de zeespiegelstijging. Ook hier zijn beeldverwerkingstechnieken, maar ook *data analytics* in het geding. Onderzoek aan dergelijke de mensheid bedreigende ontwikkelingen transcendeert de individuele belangen van een onderzoeker of zelfs onderzoekseenheid.

Zo'n positieve aanbeveling, die ver voorbijgaat aan de constatering dat er in ethische en juridische zin geen bezwaar tegen het onderzoeksvoorstel bestaat, moet worden

gezien als een advies aan het onderzoeksmanagement meer dan aan de indienende onderzoeker. De laatste heeft in beginsel altijd de vrijheid om een onderzoek niet uit te voeren.

We sluiten deze overweging over het entameren van urgent onderzoek dat de belangen van onderzoekers en betrokken instanties veruit overstijgt, af met een meer algemene vraag namelijk in hoeverre een pro-actieve rol voor een ERBI bij bepaalde typen onderzoek wenselijk is. Dit in aanvulling op de voornamelijk reactieve rol van de ERBI waarop we ons in de voorgaande hoofdstukken geconcentreerd hebben. Het zou goed kunnen dat een ERBI in een prima positie komt om ook gerichte aanbevelingen voor vruchtbaar of kansrijk onderzoek te doen. Nader onderzoek, ook in het kader van de beoogde evolutie van de ERBI werkwijze, zal moeten uitwijzen hoe een dergelijke pro-actieve rol past in het omgaan met de zorgplichten (*duty of care*) van de onderzoekers zoals behandeld in hoofdstuk 3.

5.6 Conclusies en aanbevelingen

CONCLUSIE 5.1
Ethici gebruiken morele waardetypen om de overwegingen bij ethische afwegingsprocessen te articuleren. Voorbeelden van dergelijke waarde typen zijn 'respect', 'privacy' en 'welzijn'. Er zijn echter zeer veel verschillende en uiteenlopende waarden die niet tot elkaar gereduceerd kunnen worden. Waarden kunnen ook niet eenduidig geordend worden en kunnen zelfs onderling conflicterend zijn. Dit geldt ook voor de waarden die veel voorkomen bij informaticaonderzoek. Dit zogenoemde waarde pluralisme maakt dat er geen eenduidig en vastomlijnd beoordelingskader te geven is. Van geval tot geval zal een afweging gemaakt moeten worden.

CONCLUSIE 5.2
De protocollen en richtlijnen die momenteel door veel binnen- en buitenlandse organisaties worden gebruikt bij de ethische beoordeling zijn tamelijk beperkt in scope. De vragen hebben vooral betrekking op de ethische aspecten van identificeerbare onderzoekssubjecten. Ethische aspecten van de effecten van het onderzoek op de maatschappij of milieu worden zelden meegenomen.

AANBEVELING 5.1
ERBI's wordt aangeraden om een efficiënte en transparante procedure te ontwikkelen waarbij onderscheid wordt gemaakt in een lichte en een zwaardere procedure. De lichte procedure is bedoeld voor onderzoeksvoorstellen die meer standaardonderzoek betreffen. In dit adviesrapport wordt een aanzet gedaan voor zo'n beoordelingsprocedure.

AANBEVELING 5.2

ERBI's wordt aangeraden hun besluiten goed gedocumenteerd vast te leggen en toegankelijk te maken voor onderzoekers en voor andere ERBI's. Op termijn verdient het de aanbeveling te werken aan een goed georganiseerde gezamenlijke opslag waarin alle beslissingen te raadplegen zijn. Deze centrale ontsluiting van 'moresprudentie' biedt de mogelijkheid tot het checken van consistentie en convergentie van beoordelingen en draagt bij aan de vorming van een meer eensluidend beoordelingskader.

6. WAT IS ER NOG MEER NODIG?

6.1 Inleiding

In het voorgaande deel van het advies is gesproken over het instellen van beoordelingscommissies en het opstellen van een beoordelingskader met als doel het uitvoeren van informaticaonderzoek dat ethisch en juridisch verantwoord is. Er is echter meer nodig dan beoordelingskaders en -commissies. Daar zijn meerdere redenen voor. Allereerst kan bij de uitvoering van een onderzoeksproject nog heel wat veranderen, waardoor bijvoorbeeld de inhoud van het voorstel zelf wijzigt. Voortschrijdend inzicht kan ervoor zorgen dat de koers van het project verlegd wordt of de gekozen methoden en technieken wijzigen. Ook de omstandigheden van het project kunnen wijzigen, door ontwikkelingen in de samenleving en/of de technologie. Iets wat vandaag mogelijk of gewenst is, kan in een later stadium onmogelijk of ongewenst zijn, dan wel omgekeerd. Zeker in het informaticaonderzoek doen zich voortdurend nieuwe (ethische) vraagstukken voor. In deze omstandigheden kan de initiële beoordeling van het onderzoeksproject door een beoordelingscommissie op een later moment in een ander licht komen te staan.

Een tweede reden om verder te gaan dan een beoordelingskader en een commissie die eenmalig een onderzoeksvoorstel beoordeelt, is meer psychosociaal van aard. Door in het proces voor het opstarten van een onderzoeksproject een controlemoment te introduceren wordt bevorderd dat alle aandacht uitgaat naar het succesvol passeren van dat ene controlemoment. Een geïsoleerde controleactie lokt gewenst gedrag uit voor dat moment, maar dat garandeert nog geen 'duurzaam' ethisch gedrag. Het middel van de beoordeling loopt het risico om doel op zich te worden. Dit adviesrapport wil echter juist bevorderen dat de ethische en juridische aspecten in alle fasen van het onderzoek de aandacht hebben.

Hier zou nog een derde reden aan toegevoegd kunnen worden, namelijk het belang van zorgvuldig handelen. Dat is niet alleen van belang om het imago van wetenschap hoog te houden, maar ook omdat dit aspect meegewogen kan worden als het onderzoek onverhoopt tot een claim leidt en een rechterlijke oordeel aan de orde is. Zoals in hoofdstuk 3 aangegeven hebben onderzoekers ook een zorgplicht.

In dit hoofdstuk worden enkele handreikingen gedaan om duurzaam ethisch en juridisch verantwoord gedrag in het informaticaonderzoek te bevorderen binnen de organisatie. Na enkele inzichten vanuit het omgaan met wetenschappelijke integriteit gaat de aandacht uit naar het creëren van de nodige bewustwording ten aanzien van ethische en juridische aspecten. Vervolgens worden voorstellen gedaan om deze cultuur van bewustwording te verankeren in het instituut c.q. de instelling. Dit hoofdstuk sluit af met enkele aanvullende suggesties.

Met nadruk wil de commissie erop wijzen dat het niet de bedoeling is dat nu alle aandacht en energie van een instituut gestoken wordt in de zorg voor ethische en juridische aspecten. En ook niet dat er veel meer procedures en regels bij komen. Voortdurend moet voor ogen gehouden worden dat het niet gaat om de middelen, maar om het doel, namelijk de bescherming van maatschappelijk erkende vrijheden en waarden die ook aan de orde zijn in het kader van het informaticaonderzoek. Het bewustzijn dat dit onderzoek vrijheden en waarden kan aantasten, is niet vanzelfsprekend. Daar moet dus iets voor georganiseerd worden. Dat hoort bij de maatschappelijke verantwoordelijkheid en het hoog houden van de waarde van wetenschap: claims, problemen en rampen moeten zoveel mogelijk voorkomen worden. Dit rechtvaardigt een zekere investering.

6.2 Inzichten

Voor het bewust omgaan met ethische en juridische aspecten in het wetenschappelijk onderzoek kan veel geleerd worden van de omgang met wetenschappelijke integriteit. In de afgelopen jaren is daarin terecht veel geïnvesteerd en is ook gebleken dat hier meer nodig is dan het afspreken van een code en het instellen van een klachtencommissie. Voor een duurzaam besef is een mix aan maatregelen nodig. Hieronder enkele inzichten[7]:

- Persoonlijke ethiek kan niet opgelegd worden. Morele keuzes worden door individuen zelf gemaakt.
- Ethische stellingnames en discussie kunnen wel bijdragen aan de ethische vorming van individuen.

7 Deze inzichten zijn ontleend aan een themanummer over integriteit van het *Tijdschrift voor Hoger onderwijs & Management* (2014, jaargang 21, nummer 4)

- Als ethiek geëxpliciteerd, bediscussieerd en getraind wordt, dan is internalisering en concretisering mogelijk.
- Rolmodellen, een cultuur van integriteit en duidelijk beleid dat hieraan belang hecht, zijn van wezenlijk belang voor internalisering en concretisering.
- Problemen rond wetenschappelijke integriteit vragen een voortdurend besef in alle fasen van het onderzoek.
- Het gezamenlijk opstellen van een gedragscode, regelmatige aandacht daarvoor en duidelijke handhaving ervan zijn van groot belang voor de effectiviteit en legitimatie ervan.
- Er is een sfeer nodig waarin gezegd kan worden wat gezegd moet worden.

6.3 Bewustwording

De context van het informaticaonderzoek is sterk in beweging. Bovendien interfereert dit onderzoek steeds vaker met andere domeinen, zowel in de wetenschap als in de samenleving. Dat brengt zoals in hoofdstuk 2 beschreven diverse ethische en juridische vraagstukken mee. Het lastige van juridische en – nog meer van ethische vraagstukken – is dat deze doorgaans niet gemakkelijk beantwoord kunnen worden. Dat is een van hun kenmerken. Vaak zijn er meer plausibele antwoorden mogelijk. Ethische afwegingen hebben vaak persoonlijke aspecten. En als een vraagstuk opgelost lijkt, dan doemen wel weer nieuwe vragen op.

Het stellen van de goede vragen is hier even belangrijk als het geven van de goede antwoorden, als die al eenduidig en met algemene instemming vastgesteld zouden kunnen worden. Als de goede vragen niet gesteld worden, dan liggen claims, problemen en rampen op de loer. Daarom is bewustwording en oordeelsvorming belangrijk. Belangrijk daarin is het voortdurende gesprek met anderen, het elkaar bevragen. Hoe is het ethisch bewustzijn in het eigen instituut of de instelling? Is er al eens iets voorgevallen dat achteraf bezien ethisch of juridisch niet of moeilijk te verantwoorden was? En zo ja, wat is daarvan geleerd? Zijn er naar aanleiding daarvan beslissingen genomen? Is er een gemeenschappelijk (al dan niet of gedeeltelijk vastgelegd) referentiekader van waarden en normen in het instituut? Wat staat op de agenda van de bilaterale en gemeenschappelijke overleggen? Waarover wordt (niet) vrijuit gesproken? Wat wordt als bedreigend gezien? Welke mores worden doorgegeven aan studenten en aan nieuwe onderzoekers en andere medewerkers in het instituut? Hoe wordt er tegen de (eventueel nog op te richten) beoordelingscommissie aangekeken? Is bekend waarover discussie gevoerd wordt (waarover verschil van mening is) in de beoordelingscommissie?

Als ethische en juridische aspecten van het informaticaonderzoek nadrukkelijk in beeld zijn bij zowel management als onderzoekers, als er een cultuur is van elkaar

aanspreken en bevragen, dan is het ook eerder te verwachten dat claims, problemen en schade als gevolg van het informaticaonderzoek voorkomen worden.

6.4 Verankering

Bewustwording is essentieel, maar dat gaat niet vanzelf. Het is goed om een cultuur van bewustwording te verankeren in de organisatie zodat het een onlosmakelijk onderdeel wordt van de manier van denken en werken in de organisatie. Daar zijn verschillende handreikingen voor te geven, bijvoorbeeld:

- Praat over ethische en juridische aspecten van het onderzoek in reguliere bijeenkomsten en bilaterale gesprekken. In de interactie blijkt wel dat er weinig vanzelfsprekendheden zijn als het gaat om ethische en juridische aspecten.
- Maak samen afspraken (bijvoorbeeld over de adoptie van een gedragscode of protocol).
- Stel binnen het instituut (in deeltijd) een ethisch adviseur aan voor gevraagd en ongevraagd advies en laat diegene regelmatig rapporteren over nieuwe ontwikkelingen en vraagstukken.
- Maak ethiek een verplicht onderdeel in de promotie en bij het inwerken van nieuwe medewerkers. Aan promovendi en ook aan andere onderzoekers moet duidelijk gemaakt worden dat hun onderzoek ook indirecte gevolgen voor morele waarden kan hebben.

Deze handreikingen benadrukken de gemeenschappelijkheid in het nadenken over en expliciteren van ethische en juridische aspecten en versterken het bewustzijn daarvan. Het zal bekend zijn dat het bewerkstelligen van een bepaalde cultuur tijd kost en dat voortdurende aandacht daarvoor vanuit het management een belangrijke randvoorwaarde is. Met een set afspraken en een initiële training wordt geen duurzame cultuurverandering bereikt.

Het is goed om aanvullend op de voorgaande handreikingen en aanvullend aan de beoordeling van een projectvoorstel in de aanvraag van nieuw onderzoek – bijvoorbeeld als onderdeel van de gedragscode – minimaal de volgende afspraken te maken om het voortdurend besef in alle fasen van het onderzoek levend te houden:

- In ieder onderzoeksplan staat zo nodig een ethische paragraaf en een inschatting van juridische aspecten (als vorm van risicoanalyse).
- Organiseer aanvullend op de beoordeling aan het begin van het onderzoek een mid-term check op de ethische paragraaf uit het onderzoeksplan.
- Rapporteer bij de afronding van het onderzoek over tegengekomen en nog resterende ethische en juridische vraagstukken.

Het is belangrijk dat het management van het instituut er op toeziet dat de gemaakte afspraken ook nagekomen worden, bijvoorbeeld door hiervoor aandacht te vragen in de bilaterale gesprekken en ook door het te agenderen voor de gemeenschappelijke overleggen. Dat kun je niet overlaten aan een beoordelingscommissie.

Door een cultuur van bewustwording langs genoemde lijnen te verankeren voorkom je dat het omgaan met ethische en juridische aspecten in het onderzoek verwordt tot het slechts volgen van een procedure. Er is immers ook onderzoek dat niet verloopt volgens de route: onderzoeksplan – beoordeling – honorering met subsidie. Onderzoekers moeten vanuit hun (morele) verantwoordelijkheid permanent alert zijn en zelf de afweging maken om tijdig advies in te winnen bij collega's, een daartoe aangesteld ethisch adviseur of een beoordelingscommissie.

Verankering buiten het eigen instituut

Buiten de hiervoor genoemde mogelijkheden om een cultuur van bewustzijn te verankeren in het eigen instituut, is het ook mogelijk om aansluiting te zoeken bij andere initiatieven buiten het instituut. Bijvoorbeeld door het organiseren van intervisie met andere beoordelingscommissies. Op deze manier kan het leren bevorderd worden en wordt tegelijk de kwaliteit van het onderzoek bevorderd. Het 'tegendenken' in de vorm van elkaar de goede vragen stellen, binnen en buiten de onderzoeksgroep, kan gezien worden als een vorm van 'meedenken' met als doel de kwaliteit en de uitkomsten van het onderzoek zelf te verhogen.

6.5 Conclusie

CONCLUSIE 6.1

Informaticaonderzoek en de context waarin dit wordt uitgevoerd is continu in beweging. Hierdoor doen zich rondom onderzoeksprojecten voortdurend nieuwe ethische en juridische vraagstukken voor. Eenmalig beoordelen van deze vraagstukken door een beoordelingscommissie bij de aanvang van een project is daarom niet voldoende. Onderzoeksinstituten en individuele onderzoekers moeten constant werken en uitvoering geven aan ethische bewustwording en beoordeling en dit duurzaam verankeren in de organisatie.

REFERENTIES

Breur, Tom (2013). *Big Data – de nieuwe goudkoorts*? Academic Service (SDU Uitgevers Den Haag).

CBP (2013). *CBP Richtsnoeren beveiliging van persoonsgegevens*.

Davenport, Thomas (2014). *Big Data@work: dispelling the myths, uncovering the opportunities*. Harvard Business Review Press.

Davis, Kord (2012). *Ethics of Big Data*. O'Reilly Media, Berlin.

Dijck, José van (2013). *The culture of connectivity: A critical history of social media*. Oxford University Press.

Dijck, José van (2014). *Big data, grand challenges. Over de digitalisering van het geesteswetenschappelijk onderzoek.* Clariah publication.

Dove, Edward, David Downendt et al. (2016). 'Ethics Review for International data-intensive research'. *Science*, March 2016, Volume351, Issue 6280, pages 1399-1400.

Eggers, Dave (2014). *The Circle*. Springer, Berlin.

Executive Office of the President President's Council of Advisors on Science and Technology (2014). *Report to the President: Big Data and Privacy: A Technological Perspective*.

Franssen, Maarten, Gert-Jan Lokhorst, and Ibo van de Poel (2015). 'Philosophy of technology'. *The Stanford Encyclopedia of Philosophy* (Fall 2015 Edition).

Godecharle, Simon (2014). 'De wetenschapper als koorddanser. Op zoek naar de juiste houding en het juiste gedrag.' *Tijdschrift voor Hoger onderwijs & Management* 21 (4): 14.

Grossman, Lev (2014). 'The Code War', July 21, 2014. *Time magazin*e, p.21-27.

Ham, Jeroen van der (2015). 'Embedding Ethics in System Administration Education', *Journal of Education in System Administration (JESA)*, Vol.1. Nr.1.

Hof, Chris van 't (2015). *Helpende hackers. Verantwoorde onthullingen in het digitale polderlandschap.* Ted Tok Uitgeverij.

Hoven, Jeroen Van den (2010). 'The use of normative theories in computer ethics'. *The Cambridge handbook of information and computer ethics*, pages 59-76.

Hoven, Jeroen van den, Dirk Helbing, Dino Pedreschi, et.al (2012). *The road towards ethical ICT*. CoRR, abs/1210.8181.

Jacobs, B. (2014). 'Two of the grand changes through computer and network technology'. *Privacy and Identity Management for Emerging Services and Technologies*, pages 1–11. Springer, Berlin.

Kert, Bahadir, Serhat, Cigdem Uz, Zeynep Gecu (2012). 'Scenarios for computer ethics education'. *Procedia Social and Behavioral Sciences* 46: 2706-2710.

Lane, Julia, Victoria Stodden, Stefan Bender, Helen Nissenbaum (2014). *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Cambridge University Press.

Lerouge, Inge, Gerard Cielen & Liliane Schoofs (2014). 'Goede scholing draagt bij tot permanent besef. De aanpak van KU Leuven'. *Tijdschrift voor Hoger onderwijs & Management* 21 (4): 50.

Lohr, Steve (2015a). *Data-ism: The revolution transforming decision-making, consumer behavior, and almost everything else.*
Lohr, Steve (2015b). *Dit is Big Data – Wat het is, hoe het werkt en wat het oplevert*. Maven publishing Amsterdam.
Mayer-Schönberger, Viktor and Kenneth Cukier (2014). *De Big Data revolutie: hoe de data-explosie al onze vragen gaat beantwoorden*. Maven publishing Amsterdam.
Meijers, Anthonie & Wijbo Houkes (2014). 'Kort en krachtig. De aanpak van de Technische Universiteit Eindhoven.' *Tijdschrift voor Hoger onderwijs & Management* 21 (4): 51-54.
Mols, B. (2013). *A Blow To Computer Security Research, Communications of the ACM*, October 15, 2013, http://cacm.acm.org/news/168755-a-blow-to-computer-security-research/fulltext
Morozov, Evgeny (2013). *To save everything click here*. Public affairs.
Oliver, Paul. (2010). *The student's guide to research ethics*, McGraw-Hill Education, UK
Pentland, Alex (2014a). *Social Physics: How Good Ideas Spread – The Lessons from a New Science*. Penguin.
Pentland, Alex (2014b). *Sociale Big Data: opkomst van de data-gedreven samenleving*. Maven Publishing Amsterdam.
Prins, Corien (2014). 'Handel in digitale lekken.' *Nederlands Juristenblad* 2014/865, afl. 17, p. 1171.
Schnitzler, Hans (2015). *Het digitale proletariaat.* De Bezige Bij.
Schuyt, Kees (2014). 'Leren door af te kijken. Pleidooi voor modern mentorschap'. *Tijdschrift voor Hoger onderwijs & Management* 21 (4): 9.
Spinoza, Baruch (2015). *Ethica*. Prometheus, Bert Bakker Amsterdam, vertaald en ingeleid door Henri Krop.
Stahl, Bernd C. Grace Eden b, Marina Jirotka et.al. (2014). 'From computer ethics to responsible research and innovation in ICT. The transition of reference discourses informing ethics-related research in information systems'. *Information & Management* 51 810–818.
Sullins, John (2012). 'Information Technology and Moral Values'. *The Stanford Encyclopedia of Philosophy,* ed. Edward N. Zalta.
Sunstein, Cass (2014). *Why Nudge? The politics of libertarian paternalism*. Yale University Press.
Tanner, Adam (2014). *What stays in Vegas*. PublicAffairs New York.
Verbeek, Peter Paul (2014). *Op de vleugels van Icarus*. Lemniscaat. Rotterdam.
Wynsberghe, Aimee van, Jeroen van der Ham (2015). 'Ethical considerations of using information obtained from online file sharing sites: The case of the piratebay.' *Journal of Information, Communication and Ethics in Society*, Vol. 13 Iss: 3/4, pp. 256-267.
WRR (2011). *iOverheid*, Amsterdam University Press, Amsterdam.
WRR (2011). *De staat van informatie*, WRR-Verkenning 25, Amsterdam University Press, Amsterdam.
Zevenbergen, Bendert, et al. (2015). *Philosophy Meets Internet Engineering: Ethics in Networked Systems Research.(Gtc Workshop Outcomes Paper)*. September 29, 2015.

GLOSSARIUM

De glossarium-'entries', zeer beknopt in aantal, zijn louter bedoeld om een snelle eerste indruk te krijgen of ter herinnering. We beperken ons tot termen en frasen die feitelijk in dit rapport voorkomen. Vaak zal de uitdrukking in het Engels zijn, wanneer het algemeen gebruik van een term of frase Engelstalig is. Voor een zeer uitvoerig internetsecurity-glossary zie https://tools.ietf.org/html/rfc2828. Een ander uitgebreid *Glossary of ICT terminology* is te vinden op http://www.ict4lt.org/en/en_glossary.htm . Nog een ander nuttig glossarium is http://whatis.techtarget.com/.

attack software
Deze term is grotendeels zelf-verklarend, en doelt op software die beoogt kwetsbaarheden (*vulnerabilities*) in een systeem te benutten om ongeautoriseerde toegang tot dat systeem te krijgen. Synoniem van malware, *malicious* software.

autonomous systems
i (in internettechnologie) zijn deelnetwerken van het internet, onafhankelijk van elkaar, met eigen routeringsprotocollen en adressering. Eilanden in de internet oceaan.
ii (in robotica), systemen zoals robots die autonoom kunnen functioneren in ongestructureerde omgevingen, zoals zelfbesturende auto's.

computer security, cybersecurity
Ook dit is (in eerste instantie) een grotendeels zelfverklarende term, die een inmiddels omvangrijk geworden vakgebied aanduidt. Het desbetreffende wikipedia lemma bevat een uitgebreide en informatieve lijst van aspecten van computer security, gevaren die de security bedreigen, prominente auteurs en onderzoekers op dit gebied en literatuurreferenties. Zie https://en.wikipedia.org/wiki/Computer_security.

corporate governance
betreft de aspecten en de structuur van management en bestuur van ondernemingen, de diverse processen en relaties die daarbij voorkomen, onderlinge verantwoordelijkheden van bestuurders en bestuurslichamen.

cryptography
betreft de kunst en de wetenschap van het versleutelen van informatie. De wetenschappelijke inspanning op dit gebied, met zijn grote implicaties voor privacy, maakt gebruik van diepe inzichten in de wiskunde (getaltheorie, priemgetallen, priemfactorisatie) en de zich ontwikkelende technologie van *quantum computing*.

data analytics
betreft onderzoek van 'ruwe' data in commercie en industrie om zakelijke beslissingen te onderbouwen of te verbeteren, en in de wetenschap om bestaande modellen of theorieën te toetsen. Verwant is *data-mining*, maar daarbij is het doel ab initio verborgen patronen en verbanden bloot te leggen, terwijl *data analytics* werkt met inferentie van conclusies vanuit reeds bestaande kennis.

data fusion
duidt een van de belangrijkste bedreigingen van privacy aan in de digitale maatschappij. Het betreft het aan elkaar koppelen van verschillende databases (databestanden) met persoonsgegevens, die elk op zich 'correct qua vertrouwelijkheid' zijn in de zin dat beschreven personen niet door de output van de databases zijn te reconstrueren, (te identificeren). De koppeling van zulke op zich vertrouwelijk-correcte database is dan soms op onverwachte wijze niet meer vertrouwelijk-correct. Een beroemd typisch voorbeeld is beschreven in [Lane, et al., 2014]

Dit voorbeeld betrof de koppeling van Netflix-gebruikersgegevens met IMDb, Internet Movie database met 'movie ratings'. Na de koppeling kon 96% van de Netflix-gebruikers uniek geïdentificeerd worden.

Voorbeeld 2: de koppeling van een geanonimiseerde database met sensitieve medische patiëntgegevens met een database met insensitieve gegevens.

data mining
betreft onderzoek in grote datacorpora met het oog op:

- patronen in hoe gebeurtenissen verbonden zijn, of leiden tot andere gebeurtenissen (associatie en sequentie);
- classificatie en clustering van feiten;
- voorspelling (*predictive analytics*) van toekomstige gebeurtenissen uit patronen in de waargenomen data.

Data mining wordt net als *data analytics* gebruikt in de wetenschap (wiskunde, genetica) en commercie (marktonderzoek) [Tanner, 2014].

data science
is een emergent wetenschapsgebied, voortkomend uit (o.a.) *data mining*, *data analytics*, met sterk interdisciplinair karakter, gevoed door wiskunde (in het bijzonder statistiek), informatica, patroonherkenning, kunstmatige intelligentie, *High Performance Computing*, visualisatie-technieken. Een belangrijke motor voor de opkomst van data science is het gebied van '*machine learning'* zie dit Glossarium. Toepassingen zijn legio, in biologie, economie, commercie, en de financiële wereld.

data security
is gerelateerd aan *computer security*, maar richt zich wat meer specifiek op de verdediging van data tegen aanvallers of corruptie door andere oorzaken. De verdedigingsmethoden kunnen zowel op software als hardware gebaseerd zijn.

dual use
Het *dual-use*-dilemma betreft in het algemeen technologie die voor verschillende doelen gebruikt kan worden. Meestal wordt de term gebruikt voor vreedzame versus militaire doeleinden.

embedded computing, embedded system
is een elektronische component in een groter systeem, vaak met sensoren, met een eigen microprocessor, en met een samenspel van hardware en software. Voorbeelden zijn legio in consumentenelektronica, auto's, ziekenhuisapparatuur. Zie ook http://www.esi.nl/

gaming, serious gaming
betreft een onderzoekslijn van belang voor onderwijsdoeleinden, voor de ontwikkeling van *virtual reality* en vele andere toepassingen zoals training van piloten. https://www.ou.nl/documents/10815/36320/OI_2013_2_Onderzoek_seriousgaming.pdf

human computer interaction (HCI)
betreft het ontwerp van technologie die de interactie tussen gebruiker en computer optimaliseert, gebruik makend van toepassingen ontleend aan '*cognitive science'* en aan *engineering design*, het laatste zowel software als hardware betreffend.

informed consent
Het verkrijgen van toestemming, na een heldere uitleg van implicaties en consequenties verbonden aan een onderzoek, en na constatering van een duidelijk begrip daarvan bij de proefpersoon, alvorens een proefpersoon te betrekken in een onderzoek, medisch of anderszins. Dit op basis van ethische richtlijnen die geldig zijn in het betreffende terrein, medisch of ander onderzoek, zoals in ICT.

internet of things, afkorting IoT
is het groeiende 'internetnetwerk' van objecten, voertuigen, gebouwen, *embedded systems*, opgebouwd uit hardware, software en sensoren. Een typisch (nog enigszins toekomstig) voorbeeld is de waakzame koelkast die een tekort aan een voedingsmiddel constateert en een bestelling plaatst bij de juiste winkel, terwijl de robot-stofzuiger de vloer schoonmaakt in opdracht van de afwezige bewoner, per smartphone doorgegeven.

invasive interventions
Betreft medische terminologie, interventies door chirurgische verrichtingen, in contrast met niet-invasieve interventies zonder incisies, bijv. door laparoscopie, 'medical imaging', radiotherapie, endoscopie of andere technieken.

life logging
Zie *reality mining*. Behalve de beloften die velen zien in *life logging* en *reality mining*, is er ook een bedenkelijke keerzijde, zoals betoogd door internet criticus Evgeny Morozov in zijn recente boek *To save everything click here* [Morozov, 2013]. Een nog meer bedenkelijke keerzijde wordt indringend beschreven in de dystopie van de Amerikaanse auteur Dave Eggers [Eggers, 2014].

machine learning
is een gebied in de informatica, voortgekomen uit patroonherkenning onderzoek en kunstmatige intelligentie. Het betreft analyse en ontwerp van algoritmen om data te bewerken en daaruit voorspellingen te destilleren. Typische applicaties worden gevonden in OCR, zoekmachines, computer vision. Het gebied werd ooit gedefinieerd als speciaal bedoeld om computers in staat te stellen te 'leren' zonder daartoe expliciet geprogrammeerd te zijn.

NBIC
is het acroniem voor de cluster van emergente en convergente technologieën bestaande uit nanotechnologie, biotechnologie, informatietechnologie en *cognitive science*.

New Deal on Data
Slogan van Alex Pentland, prominent theoreticus en filosoof van de Big-Data-revolutie. Volgens Pentland vormen Big Data een big deal, qua importantie vergelijkbaar met het economische en sociale New Deal programma van president Franklin D. Roosevelt, tussen 1933 en 1938, in de Verenigde Staten [Pentland, 2014a en 2014b].

reality mining
betreft het verzamelen en analyseren van data die betrekking hebben op ons sociaal gedrag, met het doel daaruit bruikbare patronen te destilleren. Het wordt mogelijk

gemaakt door de opkomst van *ubiquitous computing* met een scala van *devices*. Verwant is de term *life logging*.

responsible disclosure
term uit het gebied van *computer security*, die een voorkeursgedrag aangeeft van de ontdekkers van een kwetsbaarheid in een systeem, hieruit bestaande dat de producent voldoende tijd krijgt om de kwetsbaarheid te verhelpen voordat de ontdekkers erover publiceren. In het geval van de Radboud Universiteit Nijmegen groep die een kwetsbaarheid in de MIFARE-chip aantoonde (zie pag. 27 van dit rapport), bedroeg deze tijd ca. zes maanden. Zie ook http://www2.ru.nl/media/pressrelease.pdf en https://www.rijksoverheid.nl/onderwerpen/cybercrime/vraag-en-antwoord/responsible-disclosure.

(De tijd tussen ontdekking en reparatie van een kwetsbaarheid heeft ook te maken met de notie van een *zero day attack*: dit betreft een aanval met *attack* software op de dag zelf van de ontdekking van een kwetsbaarheid.). In plaats van '*responsible disclosure'* is ook de term *'coordinated disclosure'* in zwang.

reverse engineering is een gebruikelijke techniek met veel varianten in de analyse van hardware en software systemen, zonder het systeem zelf te modificeren, om het design en de functionaliteit van het systeem te leren kennen. Bij reverse engineering van smart cards is de analyse overigens wel destructief, de smart card wordt dan laag voor laag uit elkaar gehad.

robotics
discipline op het snijvlak van *mechanical engineering*, *electrical engineering* en *computer science*. Zie ook *autonomous systems*.

techniekfilosofie
Techniekfilosofie is een gebied in de filosofie dat onder meer de relaties bestudeert tussen technologische ontwikkelingen en ethiek, met het oog op de implicaties van technische ontwikkelingen op mens en maatschappij. Hierbij is een breed spectrum van domeinen in het geding, van wetenschappelijk onderzoek, cultuur tot politiek. Een belangrijk hedendaags inzicht is dat technologische ontwikkelingen en ethische begeleiding het beste naast elkaar, en niet na elkaar, verricht moeten worden (co-shaping) [Verbeek, 2014].

ubiquitous computing, pervasive computing, ambient intelligence
zijn namen voor de toenemende alomtegenwoordigheid van *computing devices*, anders dan de klassieke desktop computer, aanwezig in legio kleinere 'denkende objecten'. Dit kunnen intelligente koelkasten zijn, maar ook stappen- of hartslagtellers van joggers, rfid-tags en wat dies meer zijn. Verschijningsvormen worden ook gevonden in *life logging* en *reality mining*.

vulnerabilities in computer security
zijn zwaktes in een systeem die een aanvaller kan exploiteren om ongeautoriseerde toegang tot het systeem te krijgen.

wearable computing
is verwant met *ubiquitous computing*, en met *life logging*. Een definitie door enkele voorbeelden moge volstaan: Google Glass, Apple Watch en andere *smart watches*, stappentellers, *fitness trackers*.

zero day exploit
Een *zero day exploit* is in het algemeen een uitbuiting van de zwakheid in een computersysteem. Dat gebeurt vaak via een programmaatje dat speciaal is ontwikkeld om misbruik te maken van een beveiligingslek bij bijvoorbeeld een internetdienst. Het *zero day* slaat op het feit dat het een nog niet bekende zwakheid in software betreft. De zero days zijn waardevol omdat er nog geen bescherming tegen bestaat [Grossman, 2014].

AFKORTINGEN

ACM	Association for Computing Machinery
CBP	College Bescherming Persoonsgegevens
CCMO	Centrale Commissie Mensgebonden Onderzoek
CSIRT	Computer Security Incidence Response Team
CWI	Commissie Wetenschappelijke Integriteit
CW&I	Centrum voor Wiskunde en Informatica
ELSA	Ethical and Legal and Social Aspects
ERB	Ethical Review Board
ERBI	Ethical Review Board Informatics
HCI	Human Computer Interaction
ICT	Informatie en Communicatie Technologie
IEEE	Institute of Electrical Electronics Engineers
IoT	Internet of Things
KNAW	Koninklijke Nederlandse Akademie van Wetenschappen
METC	Medisch Ethische Toetsings Commissie
MKBA	Maatschappelijke Kosten Baten Analyse
MVI	Maatschappelijk Verantwoord Innoveren
NBIC	Nanotechnologie, Biotechnologie, Informatietechnologie, Cognitive Science
NSA	National Security Agency
PIA	Privacy Impact Assessment
RRI	Responsible Research and Innovation
SURF	ICT-samenwerkingsorganisatie van het onderwijs en onderzoek in Nederland
TA	Technology Assessment
TWINS	Raad voor de Technische Wetenschappen, Wiskunde, informatica, Natuur- en Sterrenkunde en Scheikunde van KNAW
VSNU	vereniging van universiteiten
WMO	Wet Mensgebonden Onderzoek

BIJLAGE 1
GESPREKSPARTNERS, REVIEWERS EN DANKBETUIGING

- Prof. dr. E.H.L. (Emile) Aarts, decaan van de faculteit Wiskunde en Informatica, Technische Universiteit Eindhoven (ten tijde van interview)
- Prof. dr. ir. H.C. (Herbert) Bos, hoogleraar Systems and Network Security, Vrije Universiteit Amsterdam
- Prof. dr. ir. J.F. (Jan Friso) Groote, hoogleraar Computer Science, Technische Universiteit Eindhoven
- Mw. Mr. (Evelijn) Jeunink, legal advisor, SURFnet
- Prof. dr. J.T. (Johan) Jeuring, hoogleraar Informatica, Universiteit Utrecht
- Prof. dr. J.N. (Joost) Kok, hoogleraar & wetenschappelijk directeur Leiden Institute of Advanced Computer Science (LIACS), Rijksuniversiteit Leiden
- Prof. dr. Ronald Leenes, hoogleraar regulation by technology, Universiteit van Tilburg
- Prof. J. (Jan) van Leeuwen, hoogleraar informatica, Universiteit Utrecht
- Prof. dr. J.J.C. (John-Jules) Meyer, hoogleraar Informatica, Universiteit Utrecht
- Prof. dr. J.B.T.M. (Jos) Roerdink, Hoogleraar (Medische) Informatica, Rijksuniversiteit Groningen
- R. (Rogier) Spoor, MSc., Manager Middleware Services, SURFnet
- Prof. dr. G.C. (Gerrit) van der Veer, hoogleraar Mens, computer, maatschappij, Open Universiteit en emeritus hoogleraar Vrije Universiteit Amsterdam
- Mw. dr. A.L. (Aimee) van Wynsberghe, assistant Professor of Philosophy of Technology at the Department of Philosophy, Ethics Advisor for the Centre for Telematics and Information Technology (CTIT), Universiteit Twente
- Wetenschappelijk Technische Raad, SURF

Reviewers

Het conceptrapport is *gereviewd* door de volgende personen:

- Prof. dr. N. (Natali) Helberger, hoogleraar Informatie recht, Universiteit van Amsterdam
- Prof. dr. C.M. (Catholijn) Jonker, hoogleraar kunstmatige intelligentie, Technische Universiteit Delft

- Prof. dr. M. (Maarten) de Rijke, hoogleraar *Information Processing and Internet*, Universiteit van Amsterdam
- Prof. dr. ir. P.P.C.C. (Peter Paul) Verbeek (UTwente), hoogleraar Filosofie van mens en techniek, Universiteit Twente

Dankbetuiging

De KNAW is de *reviewers* veel dank verschuldigd. Hun commentaren zijn zoveel mogelijk overgenomen. De *reviewers* dragen geen verantwoordelijkheid voor de inhoud van het rapport.

Onze dank strekt zich tevens uit tot bovengenoemde gesprekspartners, en tot de deelnemers aan de klankbordbijeenkomst in het Trippenhuis op 15 juni 2015. We danken daarbij in het bijzonder prof. dr. Frits Rosendaal, hoogleraar klinische epidemiologie, LUMC Leiden en prof. dr. Jaap van den Herik, hoogleraar recht en informatica, LIACS Leiden, voor hun bijdrage op deze bijeenkomst als spreker, respectievelijk discussieleider.

BIJLAGE 2
INSTELLINGSBESLUIT COMMISSIE

Het Bestuur van de KNAW, gelet op artikel 8 van het *Reglement van de KNAW*, overwegende dat door verschillende technologische en maatschappelijke ontwikkelingen de ethische, juridische en veiligheidsaspecten van informaticaonderzoek steeds belangrijker zijn geworden en dat in steeds meer wetenschapsgebieden grote – vaak privacygevoelige – gegevensverzamelingen worden gebruikt, besluit op voordracht van Adviesraad TWINS en SWR tot het instellen van de adviescommissie **Ethische, juridische en veiligheidsaspecten van big data en informaticaonderzoek**, hierna te noemen de commissie.

Artikel 1. Taakopdracht

De commissie heeft tot taak een kader te schetsen waarbinnen ethische, juridische en veiligheidsaspecten van informaticaonderzoek en daaraan gerelateerd onderzoek kunnen worden beoordeeld. Hierbij wordt in de eerste plaats gedacht aan:

- de beoordeling van onderzoek naar de beveiliging van netwerken, computersystemen en de toegang daartoe;
- het verzamelen en gebruiken van grote, vaak privacygevoelige gegevensverzamelingen (big data) zoals die in tal van wetenschapsgebieden in opkomst zijn.

Het beoogde beoordelingskader moet draagvlak hebben in het onderzoeksveld. De commissie zal daarom de relevante onderzoeksvelden bij het proces betrekken.

Gezien de breedte van de taakopdracht zal de commissie eerst de contouren van een mogelijk advies verkennen en indien nodig het onderwerp inperken. Na bespreking van deze contouren in het KNAW bestuur zal een besluit worden genomen over voortgang met een al of niet bijgestelde taakopdracht.

Artikel 2. Samenstelling en instellingsduur

Tot lid van de commissie worden op persoonlijke titel benoemd:

- Prof. dr. Jan Willem Klop (voorzitter), Vrije Universiteit Amsterdam
- Prof. dr. Jan Bergstra, Universiteit van Amsterdam
- Prof. dr. Frank van Harmelen, Vrije Universiteit Amsterdam
- Prof. dr. Jeroen van den Hoven, Technische Universiteit Delft
- Prof. dr. Bart Jacobs, Radboud Universiteit Nijmegen
- Prof. dr. Corien Prins, Universiteit van Tilburg
- Drs. Melle de Vries, KNAW

De commissie wordt ingesteld voor de duur van dit adviestraject. De commissie wordt gevraagd het rapport op te leveren voor 1 juli 2015.

De commissie wordt ondersteund vanuit het bureau van de KNAW overeenkomstig de aanwijzingen van de Algemeen Directeur.

Artikel 3. Kwaliteitsbeheer

De leden van de commissie hebben voordat zij benoemd zijn, kennis genomen van de code ter voorkoming van oneigenlijke beïnvloeding door belangenverstrengeling en de verklaring daarvan ingevuld en geretourneerd, voorafgaand aan de eerste vergadering van de commissie.

De leden van de commissie hebben kennis genomen van de handleiding adviezen en verkenningen van de KNAW zoals op 21 mei 2013 vastgesteld door het bestuur van de KNAW. Het beleid omtrent review is beschreven in bijlage B van de handleiding adviezen en verkenningen KNAW van 19 juli 2013. Van dit beleid wordt niet afgeweken.

Artikel 4. Nazorg en communicatie

De commissie besteedt aandacht aan de nazorg en communicatie rondom haar bevindingen.

Artikel 5. Kosten en vergoedingen

De leden ontvangen op basis van art. 18 lid 2 van het Reglement van de KNAW een vergoeding voor de reiskosten.

Artikel 6. Geheimhouding

De commissie neemt geheimhouding in acht ten aanzien van alle informatie die in het kader van de uitvoering van dit besluit bekend wordt en waarvan het karakter als vertrouwelijk is aan te merken.

Aldus vastgesteld door het bestuur van de Koninklijke Nederlandse Akademie van Wetenschappen op 10 februari 2014 te Amsterdam.

Namens het bestuur van de KNAW,

Dr. K.H. Chang
Algemeen directeur van de KNAW

BIJLAGE 3
VRAGENLIJSTEN, PROTOCOLLEN EN CHECKLISTS

- University of Bath, Department of Computer Science, 13-point checklist.
- University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science, Protocol for assessing the ethical permissibility of proprosed research in the Faculty of Electrical Engineering, Mathematics and Computer Science.
- University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science, Checklist for submitting a research proposal to the Ethics Committee
- University of Nottingham, School of Computer Science, Research Ethics Review Checklist
- University of Dublin, Trinity College, Faculty of Engineering, Mathematics and Science, School of Computer Science and Statistics, Research Ethics Application:
- University of Duisburg Essen, Division of Computer Science and Applied Cognitive Sciences, Faculty of Engineering, Begutachtung von Forschungsvorhaben durch die Ethikkommission der Abteilung für Informatik und Angewandte Kognitionswissenschaft, Basisfragebogen
- University of Limerick, Faculty of Science and Engineering, Research Ethics Committee, Guidelines for Research on Human Persons by Faculty or Students and the Operational Guidelines for University of Limerick Research Ethics Governance Committees
- University of Edinburgh, Research ethics checklist
- Economic and Social Research Council (ESRC), United Kingdom, Guidance for Applicants.
- European Commission, Directorate General for Research & Innovation, Guidance: How to complete your ethics self-assessement, July 2015
- Griffith University, Human Research Ethics Committee, Expedited Ethical Review Checklist
- City University London, Ethics forms and guidance documents
- Delft University of Technology, code of ethics, and project templates
- University of Amsterdam, ethical code

De volgende verwijzingen betreffen documenten en checklists die vooral op datamanagement zijn gericht.

- Data Science Association, Data Science code of professional conduct
- Boston University Libraries, Research Data Management, Overview of data management plans, templates and checklists:
- University of Auckland, Research Data Planning Checklist

BIJLAGE 4

VRAGEN VOOR EERSTE TOETSING[8]

- Is het onderzoek WMO-plichtig? Dan dient het ter toetsing aan METC te worden aangeboden.
- Wordt er in het onderzoek gebruik gemaakt van levend materiaal, levende wezens, planten, dieren, mensen, embryo's, menselijk of dierlijk weefsel? Dan dient het eventueel aan de Commissie Proefdieren te worden aangeboden.
- Wordt er in het onderzoek gebruik gemaakt van informatie of gegevens die betrekking hebben of toegepast kan worden op identificeerbare personen?
- Als het antwoord op de vorige vraag ontkennend is omdat er sprake is van geanonimiseerde gegevens is er dan een kans dat de gegevens gedeanonimiseerd kunnen worden waardoor er personen te identificeren zijn?

Bij gebruik van proefpersonen

1. Is er sprake van *informed consent*? Zijn er minderjarige proefpersonen of mensen uit kwetsbare groepen betrokken?
2. Worden de proefpersonen geconfronteerd met gevoelige onderwerpen (seksuele activiteit, drugsgebruik, verslavingen etc)?
3. Worden proefpersonen blootgesteld aan activiteiten die zij als traumatisch of genant kunnen ervaren?
4. Is het te verwachten dat het onderzoek weerstand zal oproepen bij de deelnemers vanwege aspecten gerelateerd aan etnische afkomst, geloof, geslacht, seksuele geaardheid of culturele achtergrond?
5. Worden aan de proefpersonen drugs, placebo's of andere stoffen verstrekt of worden er invasieve of anderszins potentieel gevaarlijke procedures gebruikt?
6. Worden er bloed- of weefselmonsters van de proefpersonen genomen?
7. Ervaren de proefpersonen pijn of meer dan een gering ongemak?
8. Kan het onderzoek bij de proefpersonen psychische stress, angst of onrust veroorzaken of anderszins leiden tot negatieve consequenties?

8 Afkomstig van TU Delft.

9. Moeten alle proefpersonen gedurende langere tijd op regelmatige basis worden getest?
10. Ontvangen de proefpersonen een financiële vergoeding, anders dan een redelijke vergoeding voor gemaakte kosten en tijd?
11. Als er citaten worden gebruikt van deelnemers, worden de deelnemers dan nog om toestemming gevraagd?
12. Als er fotomateriaal wordt gebruikt, worden de deelnemers dan nog om toestemming gevraagd?

Gegevensbescherming

1. Wordt in het onderzoek gebruik gemaakt van tekst dan wel geluid-, film- of video-opnames waarmee individuele personen zijn te herleiden?[9]
2. Is het doel waarvoor deze persoonsgegevens worden gebruikt expliciet gemaakt en is een grondslag voor de rechtmatigheid van het gebruik (zoals toestemming of een publiek belang) aanwezig?
3. Zijn de betrokkenen geïnformeerd dat hun persoonsgegevens worden gebruikt?
4. Worden persoonsgegevens gedeeld met landen buiten de EU?

9 Zie voor de algemene problematiek rond de persoonsgegevens ook [CBP, 2013].

BIJLAGE 5
VRAGEN OVER ONDERZOEKS-METHODE EN AANPAK[10]

Bij het gebruik van dit soort vragenlijsten is het van belang om de proportionaliteit in acht te nemen.

Algemeen

- Titel van het project
- Verantwoordelijke onderzoeker
- Uitvoerende onderzoekers
- Korte omschrijving van het project
- Plaats van uitvoering
- Namen van betrokken organisaties

Generieke vragen

- Heeft u dit of soortgelijk onderzoek al eerder ingediend bij de ERBI? (Ja/Nee)
- Zijn er externe objecten betrokken bij het onderzoek? (ja/nee)
- Zo ja, zijn de objecten van participerende onderzoek partners?
- Is de eigenaar van het object op de hoogte van het gebruik? (Ja/Nee)

Zo nee, waarom niet?

- Is er juridisch advies ingewonnen? (Ja/Nee)

Zo ja, advies graag bijsluiten.

- Zijn er disclosures afgesloten? (Ja/Nee)

Zo ja, met wie en waarover?

- Is het onderzoek publicitair gevoelig? (Ja/Nee)

Zo ja, kunt u in het kort de gevoeligheid schetsen?

10 Afkomstig van het Instituut voor Informatica, Universiteit van Amsterdam.

Domeinspecifieke vragen

Data storage

1. What are the participant/authors expectations of privacy?
2. Is the data easily searchable and retrievable? Is the data subject to open data laws or regulations?
3. Does the datas privacy policy contradict ethical principles?
4. What measures safeguard data at the site of data collection?
5. How long will the data be stored on the servers?
6. Does this contradict the time frame indicated by the researcher or institutional policies?
7. What happens to the data after the researcher completes work on the service?
8. How are the data destroyed?
9. How will cross-border data be handled if IP addresses are considered by one country to fall under privacy regulations?

Databanks

1. Where is the data stored?
2. How long will the data exist in the repository?
3. What consent is needed for subsequent data use?
4. Does the remixing/mashing of data enable identification of individual or group identities or enable any additional risks to participants?
5. In the case of shared data, what conditions were placed on data use by the original researcher, if any?
6. Regardless of conditions, what ethical responsibilities may require consideration by later users?
7. What mechanisms are in place to ensure appropriate data provenance and ownership? How will images/audio be effectively anonymized?

Security

1. Are you searching for a vulnerability in a network or application?
2. Does the owner of the information system know you are searching for vulnerability?
3. Are the activities in conflicts with regulations?
4. Which law applies? Dutch, American . . . ?
5. What is the impact of the vulnerability?
6. Does the vulnerability affects anyone privacy ?
7. How do you communicate with the owner of the vulnerability?
8. How can researcher ensure that author/participant understands and agrees that content or interaction may be used for research purposes?

9. Is the communication archived or easily searchable and retrievable?
10. Is the data subject to open data laws or regulations?
11. How long does the third party provider or ISP preserve the data and where?
12. Could privacy be achieved through anonymization of email content and/or header information?

Special interest forums

1. How do terms of service (TOS) articulate privacy of content and/or how it is shared with third parties?
2. Regardless of TOS, what are community or individual norms and/or expectations for privacy?
3. Does the author/subject consider personal network of connections sensitive information?
4. Is the data easily searchable and retrievable?
5. If the content of a subjects communication were to become known beyond the confines of the venue being studied would harm likely result?
6. Is the conversation thread or forum perceived as public or private by the author(s)/subject(s)?
7. How is profile, location, or other personally identifying information used or stored by researcher?
8. How is informed consent or protection of privacy achieved?
9. How are vulnerable persons identified and protected?
10. If non-active archives are used, how is vulnerability or harm defined and how are potential or actual subjects protected?

Social networking

1. How do the terms of service articulate privacy of content and/or how it is shared with third parties?
2. Does the author/participant consider personal network of connections sensitive information?
3. How is profile or location information used or stored by researcher? Does author/participant understand and agree to interaction that may be used for research purposes?
4. Does research purpose and design balance possible conflicts between participant and researcher perceptions of public/private and sensitive/nonsensitive?
5. Does the dissemination of findings protect confidentiality?
6. Is the data easily searchable and retrievable?
7. If the content of a subjects communication was ever linked to the person, would harm likely result?

Personal spaces

1. Could analysis, publication, redistribution, or dissemination of content harm the subject in any way?
2. If the content of a subjects communication were to become known beyond the confines of the venue being studied would harm likely result?
3. Does the author/participant consider personal network of connections sensitive information?
4. Does author/participant consider the presentation of information or venue to be private or public?
5. Do the terms of service conflict with ethical principles?
6. Is the author/subject a minor?

Virtual worlds

1. Should these virtual worlds be considered 'public'?
2. What constitutes 'privacy' in such places?
3. Should avatars be considered as persons and afforded the same protections as human subjects?
4. Will the process of requesting consent itself cause harm?
5. How and when should consent be sought?
6. What requires consent?
7. To what extent do users perceive their interactions and communication to be private in these spaces?
8. How do Terms of Service specify researcher presence, anonymity of users, and privacy/ confidentiality?
9. To what extent and in what ways could research activities interfere with or compromise a user's play or outcomes in the game?
10. How should researchers juggle their own multiple roles?
11. Could data be used to identify a user's physical location and other sensitive demographic information?

INDEX