Redactioneel

Terrorismefinanciering

Het themanummer gaat over de verschillende aspecten van en voor een effectieve aanpak van transactiemonitoring, klantacceptatie, witwassen, proliferatie en terrorismefinanciering. Zonder of met de toepassing van fintech-oplossingen en daarin betrekkend de klantbeleving en het klantgedrag. Diverse auteurs haken daarbij aan bij de (kop)zorgen en eindverantwoordelijkheid van bestuurders van financiële instellingen en waarbij de SIRA, een thematisch *risk assessment,* en het risicoprofiel van de instelling het vertrekpunt is.

Dit nummer start met de rol van de tweede lijn in post-event transactiemonitoring. **Richard Bakkers** werkt de vier verschillende rollen van de compliancefunctie verder uit: 1) Advies, waarin hij zowel de *countervailing power* als wel *consulted responsibility* verwerkt, 2) Monitoring, 3) Interne rapportage en 4) FIU reporting. Een volwassen post-event transactiemonitoring proces kent diverse *feedback loops.*

De Kerberos mag niet worden verslagen, zo stelt **Gert Demmink** in zijn artikel over het melden van ongebruikelijke transacties. Kerberos staat, als bewaker van de onderwereld, symbool voor de effectieve rol die iedereen moet spelen bij de aanpak van witwassen, proliferatie en terrorismefinanciering. Op het snijvlak van onder- en bovenwereld vinden deze illegale activiteiten plaats. De risico's manifesteren zich door middel van ongebruikelijke en verdachte transacties. Het hebben van *Fingerspitzengefühl* van de melders leidt tot het succesvol identificeren en bestrijden ervan. En dat vierentwintig (24) jaar na de invoering van de meldplicht melders kennelijk geholpen moeten worden bij het ontwikkelen van *Fingerspitzengefühl*. Dat eist een actieve informerende rol van controle- en opsporingsautoriteiten (publieke sector). Hierdoor wordt Kerberos beter beteugeld dan alleen met de focus op *auditable* processen. De ontstane passages van de onder- naar de bovenwereld moet worden bestreden.

(Ook) **Maud Bökkerink** noemt de publieke-private samenwerking. Het is efficiënter gebleken om namen en details over terrorismefinanciering te delen met instellingen. Verder beschrijft ze dat instellingen bij terrorismefinanciering op een andere manier naar transacties moeten kijken dan voor het signaleren van witwassen nodig is. Bij witwassen is met name de herkomst van het geld relevant, bij financiering van terrorisme ligt de nadruk op het doel en de bestemming van de transacties. Voor de financiering van een terrorist of een terroristische activiteit is slechts een klein bedrag nodig. Een enkele terrorist financiert zichzelf met beperkte en op het oog legale middelen. Voor de betaling van de middelen die nodig zijn om een terroristische daad uit te voeren of naar conflictgebieden af te reizen zijn geen ingewikkelde transacties nodig. Dit maakt het haast onmogelijk om een dergelijke enkelvoudige transactie met een terroristisch oogmerk te detecteren.

Verschillende maatschappelijke en politieke ontwikkelingen hebben invloed op het gedrag van klanten ten opzichte van verzekeringen. Dit uit zich vooral in een verschuiving van het collectief naar het individu. Deze veranderingen hebben effect op de verzekeringsdistributie. **Mark Arts, Anne de Groot** en **Karina Raaijmakers** richten zich op de vraag hoe veranderend klantgedrag en technologische veranderingen leiden tot veranderingen in de distributieketen van verzekeringen en hoe de komst van de Europese richtlijn verzekeringsdistributie (IDD) op het gebied van verzekeringsdistributie door deze partijen benut kan worden als kans.

Een tweetal artikelen gaan in op de mogelijkheden om innovatieve fintech-oplossingen in te zetten voor het klantacceptatieproces voor een (kosten)efficiëntere naleving van de Wwft. **Tim de Wit** behandelt uitgebreid het door de ESA's neergelegde standpunt in de '*Opinion on the use of innovative solutions by credit institutions and financial institutions in the customer due diligence process´* (kortweg: de Opinie). In de Opinie schetsen de ESA´s zeer gedetailleerde maatregelen die Wwft-instellingen moeten afwegen bij het gebruik van FinTech-oplossingen. Dankzij de Opinie ligt de weg in ieder geval open voor marktpartijen om FinTech-oplossingen te implementeren in hun klantacceptatieproces en transactiemonitoring. **Sjors van Eerten** en **Kim van Heugten** beschrijven trends waarmee de financiële criminelen voorkomen dat ze worden gedetecteerd en dat de financiële instellingen deze goed moeten doorgronden voordat deze met bijvoorbeeld fintech-oplossingen kunnen worden aangepakt. Complexiteit daarbij is de klantverwachting omtrent digitale bereikbaar- en beschikbaarheid.

Ook dit themanummer sluiten we af met de vaste rubrieken ‘De Boekenkast’ en ‘Kritisch over’.
Antoni Brack bespreekt het proefschrift over de consumentenkredietovereenkomst, welke hij kwalificeert als een heel goed proefschrift. Het bevat zowel een gedragswetenschappelijk als wel een juridisch perspectief op de overeenkomst van consumentenkrediet.
Edgar Karssing bespreekt de ethiek van kunstmatige intelligentie aan de hand van een drietal boeken, een rapport en een artikel.

Ik wens u veel leesplezier. ■

Karen Fluks
Redactie

The role of the second line of defense in post-event transaction monitoring

drs. R.W.A. Bakkers*

Trefwoorden: post-event transaction monitoring, Anti Money Laundering Directive, second line of defense

The society as a whole and regulators in specific are paying more and more attention to the negative influence of financial economic crime on the real economy. Examples of financial economic crime are money laundering, tax evasion, fraud and terrorist financing. Global money laundering transactions alone are estimated at 2 to 5% of global GDP, or roughly U.S. $1-2 trillion annually.

Financial institutions, such as banks, are exploited by criminal(s) (organizations) to proceed their illicit earnings from financial economic crime. To combat this, financial institutions are, besides other controls such as customer due diligence at onboarding, expected to dedicate an increasing amount of resources on detecting suspicious behavior[1] by their clients and to report such behavior to the government[2] without delay. Financial institutions commonly apply 'post-event transaction monitoring' to meet this obligation to detect suspicious client behavior.

A financial institution's management board is ultimately accountable for the design and operating effectiveness of post-event transaction monitoring. However, adhering the three lines of defense model[3], there are several other organizational units that play an essential role in the post-event transaction monitoring process. Examples (per line of defense) are:

- First line of defense: front-office, operations, IT, legal[4];
- Second line of defense: compliance, risk management;
- Third line of defense: internal audit.

In this article we reflect on the role of the second line of defense, and specifically on the role of the compliance function, in post-event transaction monitoring. First, we elaborate on post-event transaction monitoring from a process perspective, followed by an overview of the relevant regulatory requirements[5] and a deep-dive on the specific roles of the compliance function in post-event transaction monitoring. We finalize this article by reflecting on the impact of (new) technologies on post-event transaction monitoring and on the role of compliance and some concluding remarks.

What is post-event transaction monitoring?

As explained above, post-event transaction monitoring (in short: 'PTM') refers to an activity by which financial institutions commit themselves to detect*ing* behavior, as observed while providing services, that (may) indicate(s) financial economic crime. 'Post-event' refers to the fact that these detecting activities are initiated *after* the activity (e.g. payment or trade finance transaction) has been processed.[6] Usually, specifically for payments, all transactions are uploaded to the PTM system (software) after business hours and are analyzed by the software overnight. Transactions that are indicated as 'potentially suspicious' by the software are then added to the list of transactions that need to be analyzed in more detail as from the next business day, so-called 'alerts'.

* Richard Bakkers is a senior manager within Deloitte Risk Advisory / Regulatory Risk.

1 I.e. suspicions of financial economic crime by a client by means of payment, lending, trade finance or other transaction.

2 Usually through a dedicated 'financial intelligence unit'.

3 For instance, reference is made to IIA Position Paper 'The three lines of defense in effective risk management and control' (https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf).

4 Opinions vary by country and by financial institution on whether legal is part of the first or second line of defense.

5 Hereby we focus on EU and the Netherlands.

6 This in contrast to, for example, transaction screening performed prior to execution of transaction.

In the current regulatory environment, as further detailed in the next section, it is expected that PTM is a continuous process in which the results of a financial institution's detailed risk assessment on financial economic crime (further referred to as 'Systematic Integrity Risk Analysis' or 'SIRA') are used as input for the business rules (or: scenarios) that are used to perform PTM by means of software. Feedback loops from the operational handling of the potentially suspicious transactions (also referred to as 'alert handling') to the tuning of the software and to the SIRA ensure that the PTM process is continuously on point.

The PTM process can in our point of view be graphically summarized as follows[7]:

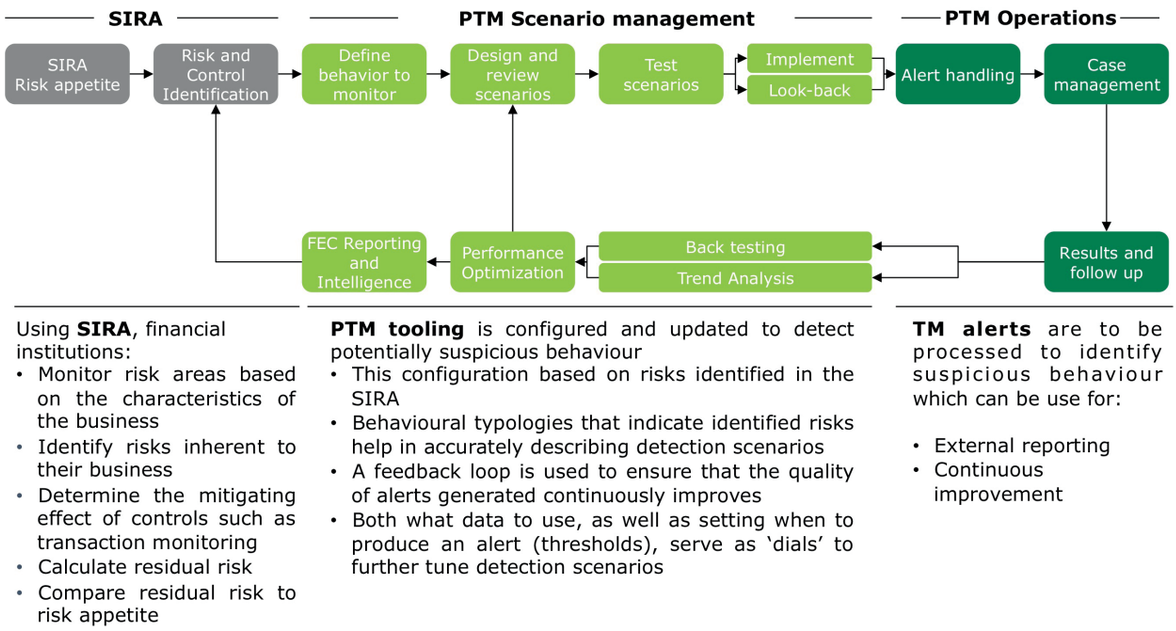


Figure 1: Elements of the post-event transaction monitoring process.

Relevant regulatory requirements

Although financial institutions should adhere as well to both civil as well as criminal codes with regard to combatting financial economic crime, for the sake of this article we focus on administrative law and its supervision by various regulators. These are:

- 4th Anti Money Laundering Directive;
- Basel Committee on Banking Supervision;
- Dutch act on the financial supervision;
- Dutch Central Bank's guidance document on (post-event) transaction monitoring.

4th Anti Money Laundering Directive

From an EU perspective, most relevant is the 4th Anti Money Laundering Directive8 (hereafter: '4AMLD'). The 4ALMD, which aims to harmonize further in the European Economic Area the combatting of financial economic crime by a wide range of financial actors, puts a heavy emphasis on employing a risk-based approach to financial economic crime at every level. It, among others, directs states to commission national risk assessments, financial institutions to conduct risk assessments[9] and to develop risk-based policies, and employees to conduct customer due diligence in a risk-based manner. The requirements from the 4AMLD should have been implemented in EU member countries' local laws and regulations by 26 June 2017.

[7] For further information please refer to: https://www2.deloitte.com/nl/nl/pages/risk/articles/approach-transaction-monitoring-program.html.

[8] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

[9] Article 8 4AMLD.

With regards to PTM specifically, the 4AMLD directs that customer due diligence measures by financial institutions include 'conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship[10]...'. Financial institutions may determine the extent of such measures on a risk-sensitive basis[11], hence our emphasis on the SIRA as explained in the previous section. The 4AMLD does not elaborate further on which specific measures are expected in terms of PTM. This is up to the individual financial institutions.

Furthermore, the 4AMLD enforces the appointment of 'a compliance officer at management level' within financial institutions.[12] This compliance officer '...shall transmit the information referred to in paragraph 1 of this Article to the FIU [financial intelligence unit] of the Member State...[13]'. Hence, the 4AMLD imposes the responsibility to report suspicious transactions to the financial intelligence unit on the second line of defense, i.e. the compliance function. The 4AMLD does not elaborate further on what is specifically expected of the compliance function in the context of combatting financial economic crime. The 4AMLD will be implemented in the Dutch act on the prevention of money laundering and terrorist financing.[14] In the implementation act 4AMLD it is mentioned[15] that the compliance function is aimed at verifying the compliance with statutory rules and internal rules which the financial undertaking has laid down. Furthermore, the compliance function has the task (i.e. responsibility) to forward the suspicious transaction reports to the financial intelligence unit.[16]

Basel Committee on Banking Supervision

Although this document dates back to April 2005 the document 'Compliance and the compliance function in banks[17]' is still often referred to as the standard work on what is expected of a compliance function within banks (its insights can be applied to other financial institutions as well). For instance, reference is made to the more recent (June 2017) Basel Committee's document 'Sound management of risks related to money laundering and financing of terrorism[18]' in which specific reference is made to the document 'Compliance and the compliance function in banks'.

In principle 7 of the document 'Compliance and the compliance function in banks' the responsibilities of the compliance function are explained to consist of:

- Advice;
- Guidance and education;
- Identification, measurement and assessment of compliance risk;
- Monitoring, testing and reporting;
- Statutory responsibilities and liaison;
- Compliance program.

Dutch act on the financial supervision

Based on this administrative law financial institutions, such as banks, are obliged to establish 'an organizational unit that exercises a compliance function in an independent and effective manner. This organizational division has the task to verify the compliance with statutory rules and internal rules that the financial undertaking [or the branch] has laid down.[19]' This act does not elaborate further on what is specifically expected of the compliance function.

Dutch Central Bank's guidance document on post-event transaction monitoring

As one of the few regulators within the EU, the Dutch Central Bank (the Netherlands) has published a very detailed guidance on what entails an adequate PTM program. The guidance document is based on the 4AMLD and the Dutch act on the prevention of money laundering and terrorist financing as well as on the Dutch Central Bank's thematic audits at banks and

[10] Article 13(1d) 4AMLD ; the term 'transaction monitoring' is not used as such in the 4AMLD.
[11] Article 13(2) 4AMLD.
[12] Article 8(4a) 4AMLD.
[13] Article 33(2) 4AMLD.
[14] Thus, the Netherlands is too late with the implementation of the 4AMLD.
[15] Article 2d(2 and 3) implementation act 4AMLD.
[16] Reference is made to article 16 of the Dutch act on the prevention of money laundering and terrorist financing.
[17] https://www.bis.org/publ/bcbs113.pdf.
[18] https://www.bis.org/bcbs/publ/d405.pdf.
[19] Article 21(1) Decree on prudential rules pursuant to the act on financial supervision.

payment providers on PTM during 2016 and 2017. The final version[20] of the guidance document was published on 30 August 2017.
The guidance document displays the PTM process as a continuous process with various feedback loops.[21] The guidance document includes a maturity model[22] containing four levels of maturity per each of the following elements:

1. SIRA/risk profile;
2. Design of AML/CFT policy;
3. TM system/business rules;
4. Alerts processing and notification process;
5. Governance: first, second and third line of defense;
6. Training and awareness.

Without going into detail on all the above elements, the guidance document, and the maturity model, explain that the basis for all PTM activities lies in a detailed risk assessment. Hence our emphasis on the SIRA as explained in the previous section.

From the list above, it is clear that the guidance document also takes the 'three lines of defense' model as a starting point. For the second line of defense specifically, the maturity model explains that to reach the minimum compliance level (indicated in orange in the maturity model) the following elements should be in place:

- Segregation of duties has been designed and exists for first, second and third line of defense;
- Responsibilities of first, second and third line of defense are adequately described;
- Second line of defense monitoring has been designed and exists. Its frequency and quality is adequate (suboptimal operating effectiveness);
- Findings from second line of defense monitoring activities are adequately followed up by the first line of defense (reactive);
- Management information about results is adequate, in essence providing direction.

Furthermore, the guidance document explains that the compliance function has an advising and (structural) monitoring responsibility.[23] In addition, the Dutch Central Bank expects from the compliance function that it pro-actively reports on its activities and on all detected shortcomings to the financial institution's senior management. The guidance document also refers to the responsibility of the compliance function to report suspicious transactions to the financial intelligence unit.

The role of compliance in post-event transaction monitoring

Overall, based on the regulatory framework as explained in the previous section and from our point of view, we have identified four areas in which the compliance function has a specific role with regard to PTM:

1. Advising;
2. Monitoring;
3. Reporting (internal);
4. Reporting to the financial intelligence unit.

These four roles, which are elaborated on in the remainder of this article, have been discussed with representatives from various market parties during a round-table session end-2017.

Advising - general

The compliance function should advise senior management on the compliance laws, rules and standards[24], including keeping them informed on developments in the area of financial economic crime related laws and regulations. In this respect, with reference to the document 'Compliance and the compliance function in banks', advising also refers to assisting senior management in preparing guidance to staff on the appropriate implementation of compliance laws, rules and standards through

[20] http://www.toezicht.dnb.nl/binaries/50-236416.pdf (only available in Dutch at this moment); a draft version of the guidance document was published in May 2017 and has been consulted by representatives from financial institutions' first and second lines of defense as well as by representatives from consulting and software firms.
[21] Please refer to page 10 (figure 1) of the Dutch Central Bank's guidance document.
[22] Please refer to pages 16 and 17 of the Dutch Central Bank's guidance document.
[23] Please refer to page 41 of the Dutch Central Bank's guidance document.
[24] With regard to financial economic crime in general and post-event transaction monitoring specifically.

policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines and in educating staff on compliance issues, and acting as a contact point within the bank for compliance queries from staff members.

With regard to education compliance should advise, among others on training topics, content development, target groups (and specific content for specific target groups) and recording of training activities and follow-up. With regard to content development, compliance should challenge that lessons learned from monitoring activities and incidents are included in the training material.

Advising - post-event transaction monitoring process

Reference is made to the graphical overview of the PTM process in this article (figure 1). Reference is also made to the widely used 'RACI' model, which describes the participation by various roles in completing tasks or deliverables for a business process. RACI is an acronym derived from the four key responsibilities most typically used: Responsible, Accountable, Consulted, and Informed.

Most closely linked to advising is the 'consulted' responsibility. There are various elements in the PTM process for which it is key that compliance is consulted (or enforces being consulted) in order for compliance to play the desired role as a second line of defense function:

- SIRA: Compliance – as a countervailing power – to challenge the input (such as data, customer segments, relevant products, etc.), throughput and output of the SIRA process and to participate in the SIRA workshops.[25] Compliance to challenge that the (inherent) financial economic crime risks are sufficiently detailed in order for the SIRA result to be useful for the design of the transaction monitoring software (business rules). Compliance to ensure that the risks associated with the development of new products and business practices, the proposed establishment of new types of business or customer relationships, or material changes in the nature of such relationships. If the financial institution has a product approval & review committee, compliance function staff should be represented on the committee and should challenge that financial economic crime risks are duly considered in the product approval (and review) process. The compliance function should also consider (new) ways to measure financial economic crime risk and use such measurements to enhance the SIRA. Technology can be used as a tool in developing performance indicators by aggregating or filtering data that may be indicative of potential compliance problems (e.g. an increasing number of customer complaints, irregular trading or payments activity, etc.);
- PTM Scenario Management:
  - Compliance to challenge the throughput and output of the so-called 'Transaction Management risk assessment'. The purpose of this assessment is to translate the SIRA financial economic crime risk scenarios into specific transaction monitoring scenarios containing information on employed modus operandi, relevant red flags and customer segments, which can be used as practical input for designing transaction monitoring scenarios (i.e. business rules);
  - Compliance to be consulted in the testing (results) of new or adjusted scenarios, lookback (procedures), backtesting and trend analysis. With regard to trend analysis the compliance function is usually also considered as one of the responsible parties to provide input for this trend analysis. The backtesting results and trend analysis insights are used to further optimize (tune) the performance of the PTM software and as input for the next SIRA;
- PTM Operations: Compliance to be consulted in case of transactions that are above a given risk threshold, for instance in case of high-risk clients, and require further investigation. It is up to the (management of a) financial institution to define the advisory role of compliance with regard to transaction monitoring.[26] Please also refer to the paragraph 'Reporting to the financial intelligence unit' below.

Monitoring

The compliance function should structurally monitor and test compliance with PTM standards by performing sufficient and representative compliance testing. A risk-based compliance monitoring[27] program is the basis for these activities. In the extension hereof, the compli-

[25] It should be clear that the first line of defense is responsible for the execution of the SIRA. A 'SIRA workshop' is mentioned as one of the possible examples to.

[26] Please refer to page 41 of the Dutch Central Bank's guidance document.

[27] In practice also referred to as 'second line monitoring'.

ance function should periodically assess the appropriateness of the bank's compliance procedures, processes and guidelines, promptly follow up any identified deficiencies, and, where necessary, formulate proposals for amendments. Furthermore, the compliance function should be involved in / initiate PTM model valuations.

Reporting (internal)

It is essential that the compliance function reports separately, independently and directly to all appropriate management levels, up to the management board, on its activities and findings. Such a compliance report includes:

- Monitoring results;
- Incidents (immediate escalation to senior management in case of major incidents);
- Results of compliance consultations as explained above under 'Advising'.

In addition to this list, reference is made to the aforementioned guidance document of the Dutch Central Bank; the Dutch Central Bank expects in the periodic compliance reporting the inclusion of management information on the main results of the financial institution's transaction monitoring.[28] Industry best practice is to arrange for (at least) a quarterly compliance reporting frequency.

Reporting to the financial intelligence unit

Reference is made to article 33(2) of the 4AMLD. In this article it is explained that the compliance officer '...shall transmit the information referred to in paragraph 1 of this Article to the FIU [financial intelligence unit] of the Member State'. This means – when taken literally – that it could be expected that the compliance function, and only the compliance function, 'pushes the button' by which a suspicious transaction report is sent to the financial intelligence unit.

There are cases in which the financial intelligence unit reports back to the financial institution or requests for (further) information. It is strongly suggested that the compliance function is the single point of contact for the financial intelligence unit in order to further guide and monitor the information flows through the financial institution.

The impact of (new) technologies

Nowadays, (new) technologies and enhanced data models are available to increase the effectiveness and efficiency of PTM. Examples are robotics, advanced analytics and artificial intelligence. These technologies can be deployed for instance for alert review preprocessing, alert risk scoring/prioritization and anomaly detection.

Without arguing the potential benefits for transaction monitoring, this also increases complexity including for the compliance function. After all, if we expect the compliance function to play a significant, predominantly advising and monitoring, role in the PTM process the compliance functions needs to be equipped to understand these (new) technologies and data models and to deploy these understandings within its activities. For instance, how can compliance establish the integrity of advanced, complex data streams that flow into the transaction monitoring system? The Dutch Central Bank is clear on this matter: 'In doing so, the organization [financial institution's senior management] should ensure that sufficient capacity – both quantitatively and qualitatively – is available [for compliance] to fulfil these roles and tasks.[29]'

Concluding remarks

In this article we have reflected on the role of compliance in PTM. We have explained that a mature PTM process is a continuous process with various feedback loops, starting from a detailed SIRA. Under pressure increased (regulatory) expectations, financial institutions, such as banks, have invested a lot in predominantly first line of defense solutions (e.g. better software, more and better opera-

[28] Please refer to page 41 of the Dutch Central Bank's guidance document.

[29] Please refer to page 41 of the Dutch Central Bank's guidance document.

tional staff to process the alerts). However, for a sustainable operating effectiveness of the PTM process, all three lines of defense should play a mature role in this process.

Based on the current regulatory expectations and industry best practices we have identified in our point of view four roles for compliance in PTM of which the most predominant in this respect are advising and monitoring. Given the increased (regulatory) expectations and complexity of the PTM process – and the impact of (new) technologies – the role of compliance in PTM is challenging and requires additional efforts and investments for the compliance function to obtain the necessary skills and tools to adequately fulfill these roles. ■

Herakles en de Kerberos

mr. G. Demmink, CFE*

Trefwoorden: Effectiviteit aanpak proliferatie- en terrorismefinanciering, witwassen, publiek-private samenwerking, informatiedeling, taskforce, toezicht De Nederlandsche Bank, nationale veiligheidsagenda, speld in de hooiberg, 'Fingerspitzengefühl'

Korte inleiding

Dit artikel gaat over een effectieve aanpak van witwassen, en proliferatie- en terrorismefinanciering.[1] De oorspronkelijke gedachte achter het melden van ongebruikelijke transacties was dat het Fingerspitzengefühl waarmee banken zich destijds op de borst sloegen, zou leiden tot kwalitatief hoogwaardige meldingen aan de FIU (toen nog MOT). In de hooiberg van transacties zouden zij feilloos de speld weten te vinden, die zou leiden tot de start van een opsporingsonderzoek. Zo is het niet gegaan. Onderzoeken en rapporten[2] wijzen op zeer geringe operationele output van het meldproces. De speld is de hooiberg geworden waarin de melders en de ontvangers van de meldingen de weg zijn kwijtgeraakt. Is er nog een koerswijziging mogelijk? Vast...

In dit artikel besteed ik geen aandacht aan de technisch-juridische aspecten van proliferatie van massavernietigingswapens en terrorisme en de financiering daarvan en evenmin aan witwassen. Die worden bekend verondersteld.

Context

Bekend is het verhaal van de Griekse held Herakles, zoon van Zeus en Alkmene, die aanvankelijk tien, later twaalf bijzonder werken kreeg opgedragen om zich te ontdoen van zijn wraakgodinnen. De geïnteresseerde lezer verwijs ik graag naar de vele publicaties over de Griekse mythen en sagen. Herakles' twaalfde werk was de ontvoering van de driekoppige hellehond Kerberos uit de onderwereld. Hij mocht deze niet doden, enkel tonen aan koning Eurystheus, zijn opdrachtgever. In mijn verhaaltje staat de Kerberos symbool voor de effectieve rol die iedereen heeft te spelen bij de aanpak van witwassen, proliferatie- en terrorismefinanciering. De scheiding tussen onder- en bovenwereld moet immers bewaard én bewaakt blijven. Op het snijvlak van onder- en bovenwereld wordt witgewassen en worden proliferatie en terrorisme gefinancierd. De Kerberos mag dus niet verslagen worden. Het beest vervult immers een rol van betekenis en mag hooguit beteugeld en getoond worden. En beteugeld wordt het! De Kerberos aan de leiband van administratieve en organisatorische tekortkomingen: uit de hiervoor genoemde rapporten (voetnoot 3) destilleer ik dat in de aanpak van het internationale witwassen '*total failure is only a decimal point away*,' dat '*many if not most of the resources devoted to AML/CFT by the financial sector have limited law enforcement or national security benefit*' en dat '*this regime* (melden van ongebruikelijke en verdachte transacties) *generates millions of suspicious transaction reports annually, however just a fraction of these lead to further investigation*.' Tenslotte: '*New 'intelligence-led' approaches to tackle financial crime are needed to achieve better outcomes. By placing emphasis on cultivating better data-sharing practices and an outcomes-focused, rather than a process-driven regime, there is enormous scope to deliver real change.*' De aanpak van het witwassen en de proliferatie- & terrorismefinanciering kan wel een stevige impuls gebruiken.

In de aanpak is de nadruk geleidelijk aan komen te liggen op auditable processes... Andere methoden om crimineel gedrag van klanten te identificeren krijgen daardoor niet de aandacht die zij verdienen, evenmin worden partijen daarvoor 'beloond'

* Gert Demmink is partner bij Philip Sidney B.V. , voorzitter van de Compliance Kamer van het Institute for Financial Crime (IFFC), lid van het Compliance Committee van FCI (voorheen Factors Chain International), voorzitter van de Overleggroep Experts Exportvergunningen van de Stichting Nederlandse Industrie voor Defensie en Veiligheid (NIDV). Hij neemt namens de NIDV deel aan de bijeenkomsten van het Export Control Committee van de AeroSpace and Defence Industries Association of Europe (ASD) in Brussel. Gert is rechter-plv. (straf en fraude) in de rechtbanken Amsterdam, Noord-Holland (inclusief Schiphol) en Limburg.

[1] Hierna: het driekoppige monster, ofwel de Kerberos, uit de Griekse mythologie. Hij is de bewaker van de onderwereld die ervoor zorgde dat de levenden deze niet konden betreden en de doden deze niet konden verlaten.

[2] – *Countering International Money Laundering: Total Failure is 'Only a Decimal Point Away'*, John A. Cassara (The Factcoalition), August 2017 (https://thefactcoalition.org/wp-content/uploads/2017/08/Countering-International-Money-Laundering-Report-August-2017-FINAL.pdf);
– *A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement*, The Clearing House, February 2017 (https://www.theclearinghouse.org/~/media/TCH/Documents/TCH%20WEEKLY/2017/20170216_TCH_Report_AML_CFT_Framework_Redesign.pdf);
– *From Suspicion to Action, Converting Financial Intelligence into Greater Operational Impact*, Europol 2017, Luxembourg, ISBN 978-92-95200-82-1.

Is alles tot nu dan vergeefs?

Sinds 1994 is – met de inwerkingtreding van de Wet melding ongebruikelijke transacties – veel gebeurd. Zo zijn bijvoorbeeld vierentwintig jaren verstreken. En zijn ongetwijfeld honderden miljoenen zo niet miljarden gespendeerd aan het optuigen van transactiemonitoring systemen, compliance afdelingen, *money laundering reporting officers*, en aan gespecialiseerde toezichtafdelingen bij de toezichthouders. In de aanpak is de nadruk geleidelijk aan komen te liggen op *auditable processes*. Elke beoordeling, afweging en beslissing moet vastgelegd worden en dus reproduceerbaar zijn. Daarmee is de nadruk komen te liggen op de kwaliteit van de risicomanagementprocessen (en daarbinnen de administratieve en organisatorische procedures en maatregelen), en minder (lees: niet) op het innovatief vermogen van zowel de melders, de ontvangers van de melders en de toezichthouders. Andere methoden om crimineel gedrag van klanten te identificeren krijgen daardoor niet de aandacht die zij verdienen, evenmin worden partijen daarvoor 'beloond'. De kritiek is dat de *examiners* geen methode hebben ontwikkeld om een dergelijke aanpak af te zetten tegen beleidsmatige of operationele tekortkomingen. Het toezichtskader schiet daarin tekort.[3]

Het wettelijke- en toezichtskader

De Nederlandsche Bank (DNB) heeft een goed toezichtskader ontwikkeld waarin de verplichtingen uit de Wet ter voorkoming van witwassen en financiering van terrorisme (Wwft) ingebed zijn. De systematische integriteitsrisicoanalyse[4] (SIRA) helpt de meldplichtige instellingen hun risico's goed in kaart te brengen en daarbij na te denken over de wijze waarop het witwas- en/of terrorismefinancieringsrisico zich kan manifesteren bij hun instelling, ofwel of bepaalde (groepen, categorieën van) transacties en/of activiteiten de instelling aanleiding geven om te veronderstellen dat ze verband kunnen houden met witwassen of financiering van terrorisme. Geen andere groep dan de financiële instellingen wordt zo goed en adequaat ondersteund met de SIRA, de daarbij behorende *guidance*, de *guidance* transactiemonitoring, de Leidraden van DNB én het ministerie van Financiën.[5] En heb ik het nog niet eens over de ondersteuning door de *Financial Intelligence Unit* (FIU), de Nederlandse Vereniging van Banken en alle andere representatieve organisaties die helpen met de interpretatie van de wet- en regelgeving en met tips voor het inrichten van de diverse bedrijfsprocessen. Als professionele financiële dienstverlener moet je dan toch wel op iets effectiefs kunnen uitkomen. En daar wringt nu net de schoen. Onvoldoende onderkend wordt nog vaak dat met het hierboven genoemde kader ondubbelzinnig vastligt op welke wijze witwas- en terrorismefinancieringsrisico's zich manifesteren. Namelijk door middel van de ongebruikelijke transactie en de verdachte transactie. Maar ook bijvoorbeeld door middel van een verzoek aan een financiële instelling van de FIU, het OM, de FIOD, een attentievestiging door een andere financiële instelling et cetera. Doet zo een situatie zich voor, dan is er volop reden voor feitenverzameling, analyse, inhoudelijke beoordeling en besluitvorming.

Onvoldoende onderkend wordt nog vaak dat met het hierboven genoemde kader ondubbelzinnig vastligt op welke wijze witwas- en terrorismefinancieringsrisico's zich manifesteren. Namelijk door middel van de ongebruikelijke transactie en de verdachte transactie

Daarnaast is er de Sanctiewet 1977 met de Regeling Toezicht Sanctiewet 1977 van DNB en de Autoriteit Financiële Markten (AFM).[6] Deze wet- en regelgeving verplichten de onder toezicht staande financiële instellingen ertoe te waarborgen dat zij op het gebied van de administratieve organisatie en interne controle maatregelen treffen ter naleving van de Sanctieregelgeving.
Die maatregelen omvatten tenminste een adequate controle van de administratie van de instelling op gesanctioneerde entiteiten zodat eventueel de financiële middelen van die relatie kunnen worden bevroren of dat voorkomen wordt dat financiële middelen of diensten ter beschikking worden gesteld aan die relatie. Als sprake is van een *hit* (de identiteit van een relatie komt overeen met een (rechts)persoon of entiteit, als bedoeld in de Sanctieregelgeving) dan meldt de instelling dit onverwijld aan de toezichthouder.

---

[3] Zie het rapport van The Clearing House, p. 5.

[4] Vindplaats: http://www.toezicht.dnb.nl/binaries/50-234068.pdf.

[5] – DNB leidraad Wfft en Sw Voorkoming misbruik financiële stelsel voor witwassen en financieren van terrorisme en beheersing van integriteitrisico's, vindplaats: http://www.toezicht.dnb.nl/binaries/50-212353.pdf.
– Ministerie van Financiën Algemene leidraad Wet ter voorkoming van witwassen en financieren van terrorisme (WWFT) en Sanctiewet (SW), vindplaats: https://www.rijksoverheid.nl/documenten/richtlijnen/2011/02/21/algemene-leidraad-wet-ter-voorkoming-van-witwassen-en-financieren-van-terrorisme-wwft-en-sanctiewet-sw.

[6] Regeling van de Autoriteit Financiële Markten en De Nederlandsche Bank NV van 1 oktober 2005 houdende regels ten behoeve van de naleving door financiële instellingen van de bij of krachtens de Sanctiewet 1977 gestelde regels met betrekking tot het financieel verkeer, vindplaats: https://www.dnb.nl/en/binaries/Regeling%20toezicht%20Sanctiewet%201977_tcm47-144737.pdf?2017103104.

Dat is overzichtelijk: ofwel de instelling meldt een ongebruikelijke of verdachte transactie ofwel (en misschien wel 'én') de instelling meldt een *hit*.

Het herkennen van transacties waarbij de instelling aanleiding heeft om te veronderstellen dat ze verband kunnen houden met witwassen of financiering van terrorisme[7] is geen sinecure en vraagt om veel inzicht en ervaring. En goede geautomatiseerde systemen.

Het herkennen van transacties waarbij de instelling aanleiding heeft om te veronderstellen dat ze verband kunnen houden met witwassen of financiering van terrorisme is geen sinecure en vraagt om veel inzicht en ervaring. En goede geautomatiseerde systemen

Inhoudelijke beoordeling transacties en besluitvorming rond melden

De crux voor een goede en effectieve melding is het op juiste wijze kunnen duiden van de feiten, de context waarbinnen deze zich voordoen in het licht van de vele witwastypologieën, proliferatie- & terrorismefinancieringstypologieën van onder meer de *Financial Action Task Force* (FATF)[8], en de Nederlandse Financial Intelligence Unit (FIU).[9] Om met Johan Cruijff te spreken: 'je gaat het pas zien als je het doorhebt.' Het herkennen van transacties waarbij de instelling aanleiding heeft om te veronderstellen dat ze verband kunnen houden met witwassen of financiering van terrorisme[10] is geen sinecure en vraagt om veel inzicht en ervaring. En goede geautomatiseerde systemen. Overigens lost blijkens de *FATF Guidance On Counter Proliferation Financing*[11] de proliferatiefinanciering zich voornamelijk op in de *targeted financial sanctions*, dus in de naleving van de Sanctiewet 1977 en de Regeling Toezicht van DNB en AFM. In de *guidance* stelt de FATF – kort gezegd – dat de Resolutie van de Veiligheidsraad van de Verenigde Naties nummer 1540 en opvolgende resoluties beogen de financiering van proliferatie-gerelateerde activiteiten van *non-state actors* tegen te gaan en dat landen controles moeten invoeren en handhaven op bijvoorbeeld financiering gerelateerd aan de export of doorvoer van items die kunnen bijdragen aan de proliferatie van massavernietigingswapens. Denk daarbij aan de zogenaamde *dual-use* goederen en technologieën en andere proliferatiegevoelige- of militaire goederen en technologieën.

....heb ik het woord *Fingerspitzengefühl* vaker gehoord dan wellicht goed is voor een mens. Deze bijzondere benaming werd door de bezigers ervan in verband gebracht met een haast onfeilbaar instinct om aan te voelen, te duiden wat niet past binnen het normale transactiepatroon van een cliënt, transacties waarvoor geen rationale valt aan te wijzen of transacties die op andere wijze opvallen

In de tijd dat ik op de Nederlandse Antillen verantwoordelijk was voor het opzetten van (toen nog) het Meldpunt ongebruikelijke transacties (MOT) en nadien bij DNB als Hoofd Expertisecentrum Integriteit medeverantwoordelijk was voor het opzetten van het anti-witwas en anti-terrorismefinancieringstoezicht (dat was allemaal tussen 1996 en 2006), heb ik het woord *Fingerspitzengefühl* vaker gehoord dan wellicht goed is voor een mens. Deze bijzondere benaming werd door de bezigers ervan in verband gebracht met een haast onfeilbaar instinct om aan te voelen, te duiden wat niet past binnen het normale transactiepatroon van een cliënt, transacties waarvoor geen rationale valt aan te wijzen of transacties die op andere wijze opvallen. Het MOT en anderen moesten durven vertrouwen op de kundigheid en vaardigheid van de melders. In dat verband is het wel aardig om in het wetsvoorstel 'Samenvoeging van de Wet identificatie bij dienstverlening en de Wet melding ongebruikelijke transacties (Wet ter voorkoming van witwassen en financieren van terrorisme) (31238)'[12] te lezen dat Heerts (PvdA) vraagt of het bij het toezicht denkbaar is dat de overheid de instellingen helpt bij het ontwikke-

[7] Ik verwijs hier enkel naar de subjectieve meldindicator omwille van het feit dat deze het lastigst is in te vullen in de praktijk.

[8] Zie de website van de FATF en de talloze publicaties: www.fatf-gafi.org.

[9] Zie de website van de FIU: https://www.fiu-nederland.nl/nl/witwas-typologieen-0.

[10] Ik verwijs hier enkel naar de subjectieve meldindicator omwille van het feit dat deze het lastigst is in te vullen in de praktijk.

[11] *FATF Guidance On Counter Proliferation Financing; The Implementation Of Financial Provisions Of United Nations Security Council Resolutions To Counter The Proliferation Of Weapons Of Mass Destruction*, February 2018, Vindplaats: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf.

[12] *Handelingen II* 2007/08, 6072, p.

len van het *Fingerspitzengefühl* dat zij soms moeten krijgen van anderen, bijvoorbeeld van opsporingsinstanties? Minister Bos antwoord daarop dat hij niet één, twee, drie ziet hoe de overheid de toezichthouder kan helpen bij het ontwikkelen van dat *Fingerspitzengefühl*. Meestal, zo stelt hij, is de toezichthouder daartoe zelf in staat bij het onderhouden van de contacten met organisaties of personen waarvan hij denkt te kunnen leren. Opvallend in deze Handelingen is dat Heerts vraagt naar een rol van de overheid en/of toezichthouder bij het ontwikkelen van dat gevoel bij de instellingen.[13] Bos reageert daarop met een verwijzing naar de overheid die de toezichthouder zou moeten helpen. Maar één ding wordt wel duidelijk uit die discussie: er moeten kennelijk partijen geholpen worden bij het ontwikkelen van het *Fingerspitzengefühl*. Aan welke zijde dan ook.

…één ding wordt wel duidelijk uit die discussie: er moeten kennelijk partijen geholpen worden bij het ontwikkelen van het Fingerspitzengefühl. Aan welke zijde dan ook. Een bijzondere instinct lijkt derhalve vereist om goed te kunnen melden. Of om de juiste besluiten te nemen om niet te melden

Succesvolle opsporing versus auditable processen

Een bijzondere instinct lijkt derhalve vereist om goed te kunnen melden. Of om de juiste besluiten te nemen om niet te melden. En die ook goed te documenteren. En daarbij dus ondersteund door talloze *guidances*, leidraden en andere hulp. Succesvolle opsporing op basis van dergelijke kwalitatief hoogwaardige meldingen zouden daarom geen nieuws moeten zijn. Toch is het dat. Ik haal twee zeer recente persberichten aan. Een Amerikaans en een Nederlands. Het Nederlandse bericht vond ik in *Het Financieele Dagblad* van 1 maart 2018: Steekpenningen. FIOD arresteert projectontwikkelaar en bouwers om corruptie en fraude. Het artikel vermeldt dat het onderzoek (naar corruptie en fraude, dus niet witwassen en proliferatie- en terrorismefinanciering[14]) is gestart na een melding bij de *Financial Intelligence Unit*.
Dan het Amerikaanse artikel. In *The Wall Street Journal* van 6 maart 2018 vond ik het bericht dat de betaling van US$ 130.000,- door de advocaat van de Amerikaanse President Donald Trump aan de *adult film actress* Stormy Daniels door de bank was gemeld als *suspicious* aan het Amerikaanse *Financial Crimes Enforcement Network*, beter bekend als FINCEN. Maar let op! De bank in kwestie ging de transactie pas onderzoeken een jaar (!) nadat deze was uitgevoerd. In het artikel wordt gesteld dat dit suggereert dat de bank in kwestie nieuwe informatie heeft ontvangen die aanleiding was om nog eens met een frisse blik naar de transactie te kijken. Aldus Charles Intriago, een voormalig federaal aanklager en witwasexpert. Hij zegt dat het wel eens zo kunnen zijn dat dat de bank in kwestie een *subpoena* (strafrechtelijke dagvaarding) of een bezoekje van de *regulators* heeft ontvangen…. Die kwamen dan zeker nog wat *Fingerspitzengefühl* bijbrengen.

Hoewel geen betrekking hebbend op een succesvolle melding van een *suspicious* transactie aan FINCEN, wil ik ook vermelden het artikel in het *Politico Magazine* van 28 februari 2018. Daarin wordt gesteld dat Paul Manafort, de verkiezingscampagne *Chairman* van de Amerikaanse President Trump, US$ 30.000.000,- zou hebben witgewassen. De auteur John A. Cassara[15] zegt dat Paul Manafort of dom, onnozel was of gewoonweg geen geluk had. De meeste witwassers komen namelijk gewoon weg met hun praktijken. Niet onbelangrijk: hij zegt dat de meeste apologeten voor het falende overheidsbeleid van mening zijn dat het allemaal gaat om *disruption* of *deterrence*, of het aantal meldingen aan de autoriteiten. Dit zijn bespottelijke gemeenplaatsen, zegt hij: '*Stopping money laundering ultimately all comes down to enforcement*.'

En wij ons allemaal maar druk maken om beleid en organisatorische en administratieve procedures en maatregelen na het uitvoeren van SIRA's. En zorgen dat alles – inclusief ieder gesprek en beslissing – gedocumenteerd is en dus *auditable*. Vooral met het oog op de integriteit van het financiële stelsel. De preventieve werking, de afschrikking. Nou, slaat u de krant maar eens na op de betrokkenheid van Nederlandse financiële instellingen bij witwassen, corruptie, omkoping en andere narigheid. Allemaal goede voorbeelden van personen en bedrijven die zich niet hebben laten afschrikken door *auditable* processen. En waarom zouden ze ook… ze komen er meestal wel mee weg.

Kort gezegd: tuig een compliance-raamwerk op, en dan kunnen we weer verder met *business as usual*…

[13] In de Handelingen wordt het woord 'instellingen' consequent gebruikt voor de financiële instellingen, de melders.

[14] Op zichzelf is dat geen probleem natuurlijk. Ongebruikelijke transacties kunnen ook duiden op corruptie of andere strafbare feiten. Dit bericht draagt juist bij aan de beeldvorming dat meldingen van ongebruikelijke transacties nauwelijks aanleiding zijn om onderzoeken in verband met witwassen of proliferatie- en terrorismefinanciering te starten.

[15] Hij is ook de auteur van het rapport van *The Factcoalition*, vermeld in voetnoot nummer 2.

De nadruk die door wetgever en toezichthouder wordt gelegd op beleid en *auditable* organisatorische en administratieve procedures en maatregelen heeft geleid tot omvangrijke en indrukwekkende compliance-raamwerken en keizerrijken. Uit een onderzoek[16] komt naar voren dat deze wel eens een averechts effect kunnen hebben op een succesvolle aanpak van witwassen, proliferatie- en terrorismefinanciering en andere vormen van financieel-economische criminaliteit. Kort gezegd: tuig een compliance-raamwerk op, en dan kunnen we weer verder met *business as usual*... Dit laatste – zo heb ik ervaren in vele gesprekken en strafzaken – wordt het beste belichaamd door de spreuk 'aan het einde van de dag, en onder de streep...' (moet er wel winst worden gemaakt). Todd Haugh, de onderzoeker en schrijver van het aangehaalde paper zegt daarover:
'*Corporate compliance is becoming increasingly "criminalized." What began as a means of industry self-regulation has morphed into a multi-billion dollar effort to avoid government intervention in business, specifically criminal and quasi-criminal investigations and prosecutions. In order to avoid application of the criminal law, companies have adopted compliance programs that are motivated by and mimic that law, using the precepts of criminal legislation, enforcement, and adjudication to advance their compliance goals. This approach to compliance is inherently flawed, however—it can never be fully effective in abating corporate wrongdoing. Criminalized compliance regimes are inherently ineffective because they impose unintended behavioral consequences on corporate employees. Employees subject to criminalized compliance have greater opportunities to rationalize their future unethical or illegal behavior. Rationalizations are a key component in the psychological process necessary for the commission of corporate crime—they allow offenders to square their self-perception as "good people" with the illegal behavior they are contemplating, thereby allowing the behavior to go forward.*'
Ongetwijfeld aanleiding voor verder onderzoek, maar op basis van enkel het bovenstaande én de vaststelling dat financieel-economische criminaliteit welig tiert in onze *financial services industry*, ondanks of juist dankzij alle inspanningen van wetgever, toezichthouders en de instellingen, meen ik dat – indachtig ook de zeer kritische rapporten genoemd in voetnoot nummer 2 – dat het roer om moet.

....op basis van enkel het bovenstaande én de vaststelling dat financieel-economische criminaliteit welig tiert in onze *financial services industry*, ondanks of juist dankzij alle inspanningen van wetgever, toezichthouders en de instellingen, meen ik dat – indachtig ook de zeer kritische rapporten genoemd in voetnoot nummer 2 – dat het roer om moet. Onze politie, andere controle- en opsporingsautoriteiten, de FIU, AIVD en MIVD en inspecties moeten actief informatie ter beschikking stellen aan financiële instellingen

Onze politie, andere controle- en opsporingsautoriteiten, de FIU, AIVD en MIVD en inspecties moeten actief informatie ter beschikking stellen aan financiële instellingen. Deze moeten daarmee aan de slag om cliënten, relaties, transacties, transactiepatronen en cliëntactiviteiten te onderzoeken en aan de hand daarvan *zinvolle* meldingen terug te doen, al dan niet gecentraliseerd via de FIU. Meldingen die leiden tot opsporing en vervolging, confiscatie van geld en goederen en internationale samenwerking daarbij. Onze wetten en beleid laten dat ook toe. Financiële instellingen mogen met vrijwaring door het OM bepaalde transacties door laten gaan *under surveillance* en daarover rapporteren aan FUI en OM. Ook het zeer recente Convenant Pilot Samewerking Bestrijding Terrorismefinanciering[17] voorziet erin dat het OM, de Nationale Politie, de FIU en de FIOD gericht informatie verstrekken aan met naam genoemde financiële instellingen: ABN AMRO Bank, ING Bank, Rabobank, De Volksbank en AEGON. De teerling is dus geworpen. Het is een eerste en veelbelovende stap op weg naar een effectieve bestrijding van financieel-economische criminaliteit die in het teken moet komen te staan van een werkelijke *risk based approach* en moedige afwegingen. Als we vaststellen dat de huidige aanpak weinig tot geen effect sorteert en dat zware criminelen met hun handelwijze eenvoudig wegkomen, dan zouden we toch op hen en hun criminele organisaties onze pijlen moeten richten. Dat impliceert dat *small fry* minder aandacht zal krijgen. Je kunt nu eenmaal niet alle ballen langdurig en succesvol in de lucht houden. Ik hoor sommigen onder u al sputteren: 'maar, dat is toch *unfair*, die krijgen dan een vrijbrief, en de integriteit van het stelsel dan...?' Leest u nog eens wat ik hierboven geschreven heb, én vooral ook de in voetnoot 2 aangehaalde rapporten. Tientallen miljoenen, misschien miljarden Euro's geven financiële instellingen uit aan 'de Wwft', aan een aanpak die niet lijkt te werken. Wat als we nou eens een deel daarvan overhevelden naar de opspoorders. Dan konden die weer alle vaardige en kundige oud-medewerkers inhuren die decennia lang de overstap maakten naar de financiële instellingen om daar – ongewild en onwetend – een bijdrage te leveren aan de *criminalization of compliance*. En daarmee wil ik niets onaardigs zeggen over alle vaardige en kundige medewerkers die nu bij de FIU en opsporingsinstanties werken. Maar het moet anders.

[16] Todd Haugh, *The Criminalization of Compliance* (March 21, 2016). 92 Notre Dame Law Review 1215 (2017); Kelley School of Business Research Paper No. 16-28. Available at SSRN: https://ssrn.com/abstract=2752621.
[17] *Stcrt.* 14 juli 2017, 39920.

Welke misdrijven, trends en bedreigingen bepalen de nationale veiligheidsagenda? Hoe kunnen financiële instellingen die verwerken in hun SIRA en op welke manier kunnen zij met gerichte informatie van genoemde partijen zinvolle feedback geven en meldingen doen?

De rol van de toezichthouder

Wat is dan straks (nog) de rol voor DNB en AFM? Die blijft onverminderd belangrijk. In mijn visie zal bijvoorbeeld DNB zijn SIRA-aanpak gaan afstemmen op de uitkomsten van het overleg met de opsporingsinstanties, FIU en OM, al dan niet binnen de FEC-Raad.[18] Welke misdrijven, trends en bedreigingen bepalen de nationale veiligheidsagenda? Hoe kunnen financiële instellingen die verwerken in hun SIRA en op welke manier kunnen zij met gerichte informatie van genoemde partijen zinvolle *feedback* geven en meldingen doen? De rol van DNB zal zich dan vooral ook moeten richten op de bewaking van het *ecosysteem* binnen en tussen[19] banken en met de genoemde autoriteiten. Is de informatie effectief afgeschermd van hen die niet gerechtigd zijn tot kennisname? Worden de interne processen en systemen voldoende effectief aangesproken om tot snel en goed resultaat te komen? Dáárop zou ik een *auditable* omgeving ingericht willen hebben, zodat de straf- en bestuursrechter in de zaken die hen worden voorgelegd, kunnen toetsen of sprake is van een rechtmatige start van het onderzoek. Duizenden scherpe spelden in plaats van warrige, onontvlechtbare hooibergen.....

Met financiële instellingen, corporates, advocaten en consultants , en ook de Nederlandse Marine, is gewerkt aan een model voor een eenduidige en uniforme aanpak voor *customer- and transaction due diligence* op de terreinen van witwassen, proliferatie- en terrorismefinanciering. Deze aanpak zal straks geïnteresseerde instellingen en ondernemingen in staat stellen hun inspanningen te ontdubbelen, te werken op basis van uniforme uitgangspunten, afspraken en processen

De rol van het IFFC

Het *Institute for Financial Crime*[20] in Den Haag – een aanjager van publiek-private samenwerking en katalysator van het gesprek tussen professionals uit de verschillende sectoren – heeft al een stukje van een nieuwe aanpak opgepakt. Met financiële instellingen, *corporates*, advocaten en consultants, en ook de Nederlandse Marine, is gewerkt aan een model voor een eenduidige en uniforme aanpak voor *customer- and transaction due diligence* op de terreinen van witwassen, proliferatie- en terrorismefinanciering. Deze aanpak zal straks geïnteresseerde instellingen en ondernemingen in staat stellen hun inspanningen te ontdubbelen, te werken op basis van uniforme uitgangspunten, afspraken en processen. Toezichthouders kunnen desgewenst meedoen of meekijken: informatie wordt beschikbaar gemaakt op basis van rollen en autorisaties. Dat de *blockchain* een rol zal kunnen spelen in de vastlegging van informatie en het delen daarvan staat buiten kijf. Maar dan moet 'de' *blockchain* wel eerst 'volwassen' en dus praktisch bruikbaar worden.

Afsluiting

De Kerberos is al een oud beestje. En sinds de tijd van Herakles zijn onder- en bovenwereld gegroeid en is de overgang daartussen zeer zeker vervaagd. Het aantal passages zal inmiddels aanzienlijk zijn. Misschien net zoveel als het aantal meldingen aan FIU's in de wereld. Het is tijd dat we de Kerberos weer eens ontvoeren en tonen aan de Koning omwille van de ontwikkeling van het *Fingerspitzengefühl*. En zorgen dat hij weer nieuw elan krijgt. Opgewassen tegen de huidige tijd en eigentijdse problemen. Maar eerst moet Herakles nog maar eens zijn vijfde werk uit de *dodekathlos* uitvoeren: het uitmesten van de Augiasstallen. Ongebruikte meldingen zijn immers net als mest: ze plakken overal aan en verstoppen het systeem. ■

[18] FEC-Raad: het bestuur van het financieel expertisecentrum. De Raad bestaat uit vertegenwoordigers op hoog niveau van DNB, AFM, FIU, Belastingdienst, FIOD, OM en de Nationale Politie.

[19] Past dat binnen de huidige privacyregelgeving en straks de AVG/GDPR? Jazeker, als we het maar goed regelen.

[20] Zie www.iffc.nl .

Terrorismefinanciering – de noodzaak van publiek-private samenwerking

mr. drs. M.J. Bökkerink*

Trefwoorden: terrorismefinanciering, publiek-private samenwerking, DNB, SIRA, NRA, FIU, transactiemonitoring, banken, betaalinstellingen, money transfer

1. Inleiding

Het is niet onbegrijpelijk dat terrorismefinanciering al een tijd hoog op de agenda staat, ook bij De Nederlandsche Bank (DNB). Zo heeft DNB in haar nieuwsbrief van januari 2018 aangekondigd dat er in 2018 bij banken en betaalinstellingen onderzoek zal worden gedaan naar terrorismefinanciering. Bijzondere aandacht zal er daarbij uitgaan naar de werking van het transactiemonitoringproces om terrorismefinanciering te voorkomen. DNB gaat er daarbij van uit dat met een adequaat transactiemonitoringproces financiële instellingen effectief de risico's op terrorismefinanciering kunnen beheersen en zo terrorismefinanciering kunnen voorkomen.[1]

Maar kunnen instellingen wel zo eenvoudig de financiering van terrorisme signaleren? Kunnen instellingen met hun transactiemonitoringssystemen 'een naald in een berg naalden' vinden? In dit artikel zal ik bekijken of de guidance van DNB over het transactiemonitoringproces instellingen helpt om via de transactiemonitoring transacties te detecteren waarbij er een vermoeden van terrorismefinanciering kan zijn. Ook zal ik kijken of er andere manieren voor instellingen zijn om op effectieve wijze terrorismefinanciering te bestrijden.

2. De SIRA

Bij de aankondiging van het themaonderzoek naar de beheersing van de risico's op het gebied van terrorismefinanciering heeft DNB diverse aandachtspunten benoemd. Zo zal DNB bekijken of instellingen de specifieke risico's om betrokken te raken bij terrorismefinanciering geanalyseerd en vertaald hebben in toereikende (beheers)maatregelen, waaronder *business rules* in het transactiemonitoringssysteem. Deze *business rules* moeten specifiek gericht zijn op het detecteren van terrorismefinanciering.

Een instelling zal allereerst in haar systematische integriteitrisicoanalyse (SIRA) moeten beoordelen wat de inherente terrorismefinancierings-risico's zijn

Om die terrorismefinancieringsrisico's te kunnen onderkennen, zal een instelling allereerst in haar systematische integriteitrisicoanalyse (SIRA) moeten beoordelen wat de inherente terrorismefinancierings-risico's zijn. De instelling zal daartoe moeten analyseren welk type van haar klanten een terrorismefinancieringsdreiging oplevert en welke producten kwetsbaar zijn voor terrorismefinanciering. De guidance van DNB over het opstellen van een SIRA geeft duidelijk weer welk proces een instelling kan volgen om een SIRA op te stellen.[2] Het is aan een instelling om ten behoeve van de organisatie-brede SIRA te bekijken of zij bepaalde soorten klanten, transacties en producten heeft. De instelling moet daarbij beoordelen in hoeverre zij de kans loopt om via deze klanten, producten of diensten bloot te staan aan terrorismefinanciering en wat de impact is als een dergelijk risico zich daadwerkelijk zou manifesteren. Aan de hand van de beoordeling van kans en impact, zal de instelling moeten beoordelen of bestaande maatregelen ter beheersing van terrorismefinanciering voldoende zijn. Een instelling kan hiervoor kijken naar de effectiviteit van de processen door te bezien of bijvoorbeeld uit de compliance-monitoring of interne audits blijkt of zich signalen of incidenten hebben voorgedaan. Indien de beheersing niet adequaat is, zal de instelling aanvullende maatregelen moeten treffen.

Een instelling zal voor het opstellen of aanpassen van de SIRA de National Risk Assessment (NRA) Terroris-

---

* Maud Bökkerink is zelfstandig consultant op het gebied van AML/CFT en sancties.

1 *DNB Nieuwsbrief Banken d.d. 31 januari 2018*, https://www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-banken/NieuwsbriefBanken-januari2018/dnb371920.jsp.

2 DNB, 'De integriteitrisicoanalyse, meer waar dat moet, minder waar dat kan', http://www.toezicht.dnb.nl/binaries/50-234068.pdf.

mefinanciering kunnen gebruiken.[3] Daarnaast kan een instelling ook de zogeheten *Supranational Risk Assessment* (SNRA) van de Europese Commissie gebruiken om te bekijken welke risico's relevant kunnen zijn.[4]

De NRA benoemt als terrorismefinancieringsrisico's in Nederland onder andere financieringen via virtuele valuta, via prepaid-, debet-, of telefoonkaarten, leningen en giften van familie of vrienden en financiering uit eigen middelen. Ook wordt geld dat komt van (buitenlandse) stichtingen of van non-profit organisaties als terrorismefinancieringsrisico genoemd.

In de Europese SNRA wordt nagegaan in welke omstandigheden de diensten en producten die de Europese financiële sector aanbiedt of levert, misbruikt kunnen worden om terrorisme te financieren. Met betrekking tot terrorismefinanciering worden onder andere als kwetsbare diensten of producten genoemd elektronisch geld, geldtransferdiensten, crowdfundingplatforms, virtuele valuta's, consumentenkredieten en kleine leningen. En ook in de SNRA wordt van non-profit organisaties aangegeven dat deze kwetsbaar zijn voor terrorismefinanciering.

Indien bij het opstellen van de SIRA bijvoorbeeld uit de interne data-analyse van het soort klanten blijkt dat er meer non-profit organisaties dan verwacht in het klantenbestand zitten waarbij zich een terrorismefinancieringsrisico kan manifesteren, zal de instelling moeten beoordelen of de beheersmaatregelen wel voldoende zijn of dat extra maatregelen getroffen moeten worden om mogelijke terrorismefinancieringsrisico's te beheersen. En het ligt in de verwachting dat DNB zal kijken of dergelijke risico's ook adequaat in het transactiemonitoringssysteem zijn verwerkt.

3. De transactiemonitoring

Uit de DNB guidance over transactiemonitoring komt naar voren dat DNB verwacht dat een instelling specifieke indicatoren voor terrorismefinanciering vertaald heeft in business rules en deze rules vervolgens in het transactiemonitoringssysteem opgenomen heeft.[5] Daarbij geeft DNB aan dat alleen transactielimieten niet volstaan, aangezien uitsluitend een laag transactiebedrag niet duidt op terrorismefinanciering. DNB stelt daarbij dat banken business rules over transactielimieten moeten koppelen aan andere indicatoren van terrorismefinanciering, bijvoorbeeld lagere grensbedragen voor transacties met risicolanden of regio's in samenhang met bepaald soorten cliënten, zoals stichtingen.

DNB heeft voor betaaldienstverleners grotendeels vergelijkbare guidance uitgegeven.[6] Voor de betaaldienstverleners geeft DNB aan zich ervan bewust te zijn dat terrorismefinanciering voor betaaldienstverleners lastiger is te detecteren dan bijvoorbeeld voor banken aangezien banken meestal over meer informatie beschikken. DNB verwacht echter ook dat betaaldienstverleners specifieke indicatoren voor terrorismefinanciering vertaald hebben in business rules en die vervolgens in hun transactiemonitoringssystemen opgenomen hebben.

In haar guidance verwijst DNB naar indicatoren voor terrorismefinanciering, bijvoorbeeld risicolanden of regio's of bepaalde soorten klanten zoals stichtingen, reisbureaus, webshops waar chemicaliën worden verkocht, crowdfunding platformen en e-currency (bitcoin)-handelaren. Vraag is of instellingen hier voldoende aan hebben om een SIRA te maken en op basis daarvan concrete business rules op te stellen. Daarbij speelt ook een rol dat uit de guidance niet goed naar voren komt dat het (anders dan bij witwassen) bij de financiering van terrorisme niet zo zeer om de herkomst van het geld gaat, maar om het doel waarvoor het geld wordt gebruikt en door wie het wordt gebruikt.[7] Instellingen moeten bij terrorismefinanciering op een andere manier naar transacties kijken dan voor het signaleren van witwassen nodig is. Bij witwassen is met name de herkomst van het geld relevant, bij financiering van terrorisme ligt de nadruk op het doel en de bestemming van de transacties.

3.1 De vierde anti-witwasrichtlijn

Naast de guidance van DNB zou een instelling bij het transactiemonitoringproces ook gebruik kunnen maken van bijlage III bij de vierde anti-witwasrichtlijn.[8] In deze bijlage worden risicoverhogende factoren genoemd waar een instelling ten minste rekening mee moet houden bij het cliëntenonderzoek (waaronder de voortdurende controle en dus ook de transactiemonitoring).[9] De in die bijlage genoemde cliëntgebonden risicofactoren als ook de product-, dienst-, transactie- of

---

[3] Wetenschappelijk Onderzoek- en Documentatiecentrum, 'National Risk Assessment Terrorismefinanciering', *Cahier* 2017-14.

[4] Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, 26 juni 2017.

[5] DNB, Guidance Post-event transactiemonitoringsproces bij banken, paragraaf 5.3.2.

[6] DNB, Guidance Post-event transactiemonitoringsproces bij betaaldienstverleners, paragraaf 5.3.3.

[7] https://www.fiu-nederland.nl/nl/over-fiu/wat-is-terrorismefinanciering.

[8] Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie.

[9] Zie ook art. 8 lid 2 wetsvoorstel Implementatiewet vierde anti-witwasrichtlijn, *Kamerstukken II* 2017/18, 34 808, nr. 2.

leveringskanaalgebonden risicofactoren lijken niet of nauwelijks relevant om terrorismefinanciering te kunnen detecteren. Alleen met betrekking tot de geografische risicofactoren is de factor 'landen die financiering of ondersteuning verschaffen voor terroristische activiteiten, of op het grondgebied waarvan als terroristisch aangemerkte organisaties actief zijn' relevant. Vraag is wat er wordt bedoeld met 'op het grondgebied waarvan als terroristisch aangemerkte organisaties actief zijn'. Immers, ook in vele landen van de EU zijn terroristische organisaties actief. Betekent dit nu dat instellingen landen als België, Frankrijk, Spanje en het Verenigd Koninkrijk – landen waar de afgelopen jaren terroristische aanslagen hebben plaatsgevonden – als verhoogd risico voor terrorismefinanciering moeten beschouwen. Vanuit de richtlijn wordt hier geen verdere duiding aan gegeven.

3.2 De FATF

Ook is het belangrijk dat een instelling kennis neemt van de informatie die de Financial Action Task Force (FATF) publiceert. Het onderwerp terrorismefinanciering is al sinds 2001 een prioriteit voor de FATF, met een intensivering sinds 2015 door de verhoogde terroristische dreigingen.[10] De FATF heeft de afgelopen jaren meerdere rapporten gepubliceerd over terrorismefinanciering.[11] Deze rapporten geven veel informatie over de methoden die worden gebruikt om terrorisme te financieren, zoals de criminele activiteiten waarmee geld wordt vergaard, het gebruik van non-profit organisaties om geldstromen te legitimeren, en bancaire overboekingen, cash en money transfers om geld te verplaatsen. Instellingen kunnen hier zeker hun kennis mee verrijken en de SIRA mee voeden. Echter, de informatie is doorgaans niet gedetailleerd genoeg om er daadwerkelijk scenario's en detectieregels van te maken voor het transactiemonitoringssysteem.

Naast het financieren van terroristische activiteiten, is recentelijk ook het financieren ten behoeve van rekrutering voor terroristische doeleinden onder de aandacht gebracht. De FATF heeft hierover in januari 2018 een rapport gepubliceerd.[12] In dit rapport staan als belangrijkste financieringsbronnen van terroristische rekrutering onder andere financiële steun van terroristische organisaties, donaties en crowdfunding, misbruik van non-profits en opbrengsten uit criminele activiteiten. Ook de methoden die in dit rapport staan beschreven, kunnen instellingen gebruiken om de activiteiten en transacties van de klanten te controleren op terroristische doeleinden.

De gegeven guidance over terrorismefinanciering is veelal te generiek om tot concrete indicatoren en business rules ten behoeve van het transactiemonitoringssysteem te komen

4. Verschillen in terrorismefinanciering

Zoals hierboven geschreven is de gegeven guidance over terrorismefinanciering veelal te generiek om tot concrete indicatoren en business rules ten behoeve van het transactiemonitoringssysteem te komen. Daarbij komt in de guidance slechts beperkt naar voren dat het financieren van een enkele terrorist of een enkele terroristische daad verschillend zal zijn van de financiering van een terroristische groepering of organisatie. Er wordt in de diverse guidance documenten geen rekening mee gehouden dat terrorismefinanciering ziet op het financieren van een individuele terrorist, een terroristische activiteit maar ook een terroristische organisatie. Dit terwijl FATF Recommendation 5 stelt dat:

'Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention[13], and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts.'

Voor de financiering van een terrorist of een terroristische activiteit is slechts een klein bedrag nodig. Een enkele terrorist financiert zichzelf met beperkte en op het oog legale middelen (salaris, uitkeringen, spaargeld, krediet).[14] Voor de betaling van de middelen die nodig zijn om een terroristische daad uit te voeren of naar conflictgebieden af te reizen zijn geen ingewikkelde transacties nodig. De transactie zal dan ook bestaan uit een of een aantal enkelvoudige, lineaire overboekingen: een betaling van A naar B.

Een dergelijke transactie is in vergelijking met witwastransacties niet gecompliceerd en wellicht daarom ook niet met de huidige transactiemonitoringssystemen eenvoudig te detecteren. Voor een transactiemonitoringssysteem ziet een dergelijke transactie er niet anders uit dan menig andere 'gewone' overboeking. Dit maakt het haast onmogelijk om een dergelijke enkelvoudige transactie met een terroristisch oogmerk te detecteren.

Bij witwassen gaat het daarentegen om 'circulaire' geldbewegingen. De crimineel wil immers zijn illegaal verkregen geld terug en zal daarom via complexe zake-

[10] http://www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html.

[11] FATF, *Terrorist Financing in Central and West Africa, oktober 2016; Emerging Terrorist Financing Risks, oktober 2015; Financing of the Terrorist Organisation Islamic State in Iraq and the Levant, februari 2015; Risk of Terrorist Abuse in Non-Profit Organisations*, juni 2014.

[12] FATF, *Financing of Recruitment for Terrorist Purposes*, januari 2018.

[13] International Convention for the Suppression of the Financing of Terrorism, Adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999.

[14] Mara Wesseling, 'Een effectief beleid tegen terrorismefinanciering: tijd voor een eerlijk gesprek', in: *De Compliance Officer* 2018, nr. 2, Nederlands Compliance Instituut.

lijke structuren, verschillende bankrekeningen en overboekingen via meerdere landen, proberen zijn criminele geld een schijn van legale herkomst te geven om het uiteindelijk weer zelf te kunnen gebruiken.

Ook is er verschil tussen de financiering van een enkele terrorist of terroristische daad en de financiering van een terroristische organisatie. Over het algemeen zijn de financieringsbehoeftes om de infrastructuur, personeel en activiteiten van een (grote) terroristische organisatie te onderhouden zeer hoog.[15] Daarbij verkrijgt een terroristische organisatie zijn inkomsten uit criminele activiteiten, zoals drugsproductie en -handel, afpersing en (mensen) smokkel. Een terroristische organisatie zal daarom meer op een witwasorganisatie lijken omdat ook voor deze inkomsten de herkomst van de gelden zal moeten worden verhuld. Banken kunnen daar op monitoren, op vergelijkbare wijze als voor witwassen.

De verwachtingen van DNB die uit de guidance blijken zullen dan ook zeker relevant zijn voor het detecteren van de geldstromen van een terroristische organisatie omdat daar dezelfde of vergelijkbare scenario's zullen gelden als voor witwassen.

Maar een enkele terrorist die zichzelf financiert of die door een familielid wordt gefinancierd zal, zonder informatie uit andere, open bronnen, niet met het transactiemonitoringssysteem zijn te vinden. Hier is maatwerk nodig en eventueel handmatige analyses. Zo is het voor te stellen dat wanneer een persoon op de nationale sanctielijst terrorisme[16] wordt geplaatst, een instelling – bij een positieve hit – de transactiehistorie van die persoon zal analyseren om vast te stellen of er mogelijke transacties hebben plaatsgevonden waarbij de instelling een vermoeden van terrorismefinanciering kan hebben. Ook zal de instelling kunnen analyseren of er mogelijk ongebruikelijke transacties van personen die op hetzelfde adres wonen of van familieleden hebben plaatsgevonden. De FIU heeft een casus hierover op haar website staan:

'Een man had gedurende een periode van ruim een jaar geld overgemaakt naar zijn broer die was uitgereisd naar Syrië om aan de zijde van Islamitische Staat mee te vechten. In totaal maakte de man hiervoor zo'n 17.000 euro over. Een aantal van deze transacties naar Syrië was uit een analyse van de FIU-Nederland naar boven gekomen. Toen de broer op de sanctielijst van de Verenigde Naties was geplaatst wijzigde de man zijn tactiek en liet anderen de overboekingen uitvoeren.'[17]

4.1 Netwerkanalyses

In DNB's guidance 'Post-event transactiemonitoringsproces bij money transfer organisaties' wordt gesteld dat money transfer organisaties met behulp van het transactiemonitoringssysteem transactiepatronen of netwerken en combinaties van transacties kunnen detecteren.[18] DNB denkt hierbij aan een samenstel van transacties van een of meerdere cliënten die op geaggregeerd niveau op terrorismefinanciering (kunnen) duiden. DNB verwacht van money transfer organisaties dat zij gebruik maken van netwerkanalyses om de effectiviteit van de transactiemonitoring te vergroten. De netwerkanalyses zouden de mogelijkheid kunnen bieden om (geautomatiseerd) standaard bredere transactiepatronen en -structuren en netwerken van transacties te detecteren.

De plicht om een dergelijke uitgebreide analyse te maken, kan ook worden afgeleid uit het voorgestelde art. 8 lid 3 Implementatiewet vierde anti-witwasrichtlijn: 'een instelling neemt redelijke maatregelen om alle complexe en ongebruikelijk grote transacties en alle ongebruikelijke transactiepatronen die geen duidelijk economisch of rechtmatig doel hebben te onderzoeken en onderwerpt de gehele zakelijke relatie met de cliënt in dat geval aan een verscherpte controle.'

Indien een instelling stuit op een transactie die duidt op terrorismefinanciering, moet de gehele zakelijke relatie met een cliënt door de instelling aan een verscherpte controle worden onderworpen. Daarbij gaat het niet alleen om een controle van de in het kader van de zakelijke relatie verrichte transacties, maar moeten er ook verscherpte maatregelen worden getroffen en een meer intensieve transactiemonitoring.[19]

Dit soort netwerkanalyses zullen echter niet standaard in de transactiemonitoringssystemen van banken zitten. Hier zijn slimme(re) systemen voor nodig. Daarbij is het eenvoudiger om een dergelijk netwerk achteraf in kaart brengen, bijvoorbeeld nadat een persoon op de nationale sanctielijst is geplaatst of wanneer er informatie in de pers verschijnt. Zonder aanvullende kennis over een persoon is vooraf niet te detecteren of een persoon een transactie uitvoert met het oogmerk een terrorist of een terroristische daad te financieren.

5. Noodzaak van andere bronnen

Zoals hierboven aangegeven is voor verder onderzoek informatie uit andere, open bronnen noodzakelijk. Zo noemt DNB het een good practice als een instelling signalen uit de pers goed volgt.[20] Uit de jurisprudentie blijkt dat instellingen dat ook doen.

Uit de uitspraak van Rechtbank Amsterdam 7 maart 2018[21] komt naar voren dat een bank naar aanleiding

---

[15] FATF, *Emerging Terrorist Financing Risks*, oktober 2015, p. 9.
[16] https://www.rijksoverheid.nl/documenten/rapporten/2015/08/27/nationale-terrorismelijst.
[17] https://www.fiu-nederland.nl/nl/levensonderhoud-van-een-is-medestrijder.
[18] DNB, Guidance Post-event transactiemonitoringsproces bij money transfer organisaties, paragraaf 5.3.4.
[19] Memorie van Toelichting bij de Implementatiewet vierde anti-witwasrichtlijn, *Kamerstukken II* 2017/18, 34 808, nr. 3, p. 55.
[20] DNB, Guidance Post-event transactiemonitoringsproces bij banken, p. 35.
[21] ECLI:NL:RBAMS:2018:1303.

van negatieve berichten over een stichting in de pers onderzoek heeft gedaan naar de klantrelatie met de stichting, om na te gaan of die relatie integriteits- of reputatierisico's mee kon brengen. De bank had de stichting regelmatig verzocht om informatie over bepaalde transacties op de bankrekeningen, onder andere over contante stortingen en over een aantal overschrijvingen naar de bankrekening van een andere stichting onder vermelding van 'lening'. Ook waren er forse bedragen uit Koeweit ontvangen door de stichting, in het bijzonder van de International Islamic Charitable Organization, die in diverse mediaberichten in verband werd gebracht met radicaal-extremistische organisaties. De rechtbank oordeelde dat de bank op diverse gronden aanwijzingen had dat de stichting, in elk geval in de publiciteit, negatief werd geassocieerd met terrorisme en witwassen. De rechtbank stelde daarbij dat van een bank in beginsel niet kan worden verlangd dat zij een diepgaand onderzoek instelt naar de juistheid van dergelijke beschuldigingen. Wel kan van de bank worden verlangd dat zij die beschuldigingen, behoorlijk onderbouwd en toegelicht, aan de cliënt voorhoudt, maar hieraan had de bank in deze casus voldaan.

Dit is echter allemaal achteraf, als er al in publieke bronnen informatie over personen of entiteiten verschijnt. Echter, bij de bestrijding van financiering van terrorisme speelt het *voorkomen* van delicten ook een grote rol speelt vanwege de ontwrichtende gevolgen van een terroristische aanslag.[22]

Als er vanuit de overheid de wens is om direct een mogelijke terrorismefinancieringstransactie te detecteren – en die wens is er anders zou er op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) geen eis zijn om onverwijld vermoedens van terrorismefinanciering te melden – dan moet er ook een informatiestroom vanuit de overheid richting banken en andere Wwft-plichtige instellingen zijn. En voor een aantal banken gebeurt dat ook.

Het is veel efficiënter gebleken om namen en details over terrorismefinanciering te delen met instellingen

5.1 Publiek-private samenwerking

Het is veel efficiënter gebleken om namen en details over terrorismefinanciering te delen met instellingen. Op grond van art. 18 Wet politiegegevens is dat ook mogelijk en wordt daar ook gebruik van gemaakt. Daar is natuurlijk wel vertrouwen tussen partijen voor nodig maar na 25 jaar meldplicht moet deze er wel zijn.

FIU-Nederland geeft aan dat het detecteren van ongebruikelijke transacties die te relateren zijn aan terrorismefinanciering specifieke kennis vereist en dat goede samenwerking met instellingen onontbeerlijk is. De FIU wisselt binnen het terrorismefinancieringsplatform met de financiële sector informatie uit. Door FIU-Nederland ontwikkelde risicoprofielen worden met een aantal geselecteerde instellingen gedeeld om hen zo goed mogelijk te voorzien van mogelijkheden geldstromen te analyseren op aan mogelijke terreurfinanciering gelieerde transacties. Dit leidt regelmatig tot nieuwe meldingen van ongebruikelijke transacties. Transacties uitgevoerd door zogenaamde uitreizigers worden zo gedetecteerd en aan relevante Nederlandse overheidsdiensten verstrekt bij de bestrijding van terrorisme.[23, 24]

Bij de FIU heeft de samenwerking duidelijk effect. Uit het Jaaroverzicht 2016 komt naar voren dat in 2016 door de FIU-Nederland, 4.494 transacties verdacht zijn verklaard omdat deze op basis van analyse een verband hielden met het financieren van terrorisme, onderzoeken naar contraterrorisme of de uitreis naar Syrië en/of Irak. Dit heeft geresulteerd in 623 dossiers, wat meer dan een verdubbeling was in vergelijking met 2015.[25]

Ook is in juli 2017 het 'Convenant Pilot Samenwerking Bestrijding Terrorismefinanciering' gepubliceerd. Deze samenwerking tussen een aantal grootbanken, de FIU-NL en de opsporingsautoriteiten heeft tot doel informatiedeling mogelijk te maken om zo terrorismefinanciering te voorkomen en op te sporen. Binnen deze pilot wordt tussen convenantpartners relevante informatie gedeeld. In de overwegingen staat dat 'door het gericht verstrekken van informatie door de publieke partijen worden de private partijen beter in staat gesteld om binnen de eigen systemen en in samenwerking met elkaar dergelijke relevante transacties te identificeren, deze in kaart te brengen en als ongebruikelijk te melden aan FIU-NL, zoals wettelijk verplicht.'

Ook internationaal is de trend te zien dat, om betere meldingen bij FIU's te krijgen, er publiek-private samenwerking nodig is. Zo is in oktober 2017 is het rapport 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime' gepubliceerd waarin de efficiency, effectiviteit en proportionaliteit van de meldsystemen aan de orde is gesteld. In dit rapport van Nick Maxwell en David Artingstall is een aantal 'public–private financial information-sharing partnerships' onderzocht en vastgesteld dat deze aanpak effectiever kan zijn om financieel-economische criminaliteit aan te pakken.[26]

Ook de FATF stelt dat '*the private sector and civil society show a strong willingness to assist authorities in terrorist financing issues. However, in many situations, financial*

[22] https://www.fiu-nederland.nl/nl/over-fiu/wat-is-terrorismefinanciering.
[23] FIU Nederland Jaaroverzicht 2016, paragraaf 5.2, p. 29.
[24] https://www.fiu-nederland.nl/nl/mogelijke-terreurfinanciering.
[25] FIU Nederland Jaaroverzicht 2016, paragraaf 5.3, p. 31.
[26] https://rusi.org/publication/occasional-papers/role-financial-information-sharing-partnerships-disruption-crime.

institutions are likely to have difficulty in identifying relevant transactions without close interaction with law enforcement agencies or FIUs.'[27] De FATF geeft aan dat instellingen contextuele informatie nodig hebben om de geldstromen die gerelateerd zijn aan terroristische activiteiten te identificeren.

Dit betekent natuurlijk niet dat banken achterover kunnen zitten en wachten tot de publieke kant met informatie komt. Instellingen zouden zeker slimmere transactiemonitoringssystemen moeten ontwikkelen. De huidige systemen met statische business rules en scenario's die zelden of nooit aangepast worden leveren dagelijks vele alerts op die onderzocht moeten worden. Maar medewerkers hebben niet altijd die informatie die nodig is om een goed onderzoek te doen. Met specifieke, gerichte informatie van opsporingsautoriteiten zouden die transacties onderzocht en gemeld kunnen worden waar de opsporing echt behoefte aan heeft. Naast slimmere transactiemonitoringssystemen zit een oplossing dus zeker in het uitwisselen van informatie tussen opsporing en private partijen.[28]

6. Conclusie

DNB verwacht dat instellingen met business rules in het transactiemonitoringssysteem die specifiek gericht zijn op het detecteren van terrorismefinanciering, effectief terrorismefinancieringsrisico's kunnen beheersen. Hierbij wordt onderschat dat een systeem dat gebouwd is om witwassen te bestrijden niet eenvoudig is om te bouwen en aan te passen naar een systeem om terrorismefinanciering te detecteren. Zeker niet daar waar het gaat om de financiering van een enkele terrorist of terroristische activiteit.

Het is uit informatie van de FIU en het feit dat er een convenant is tussen publieke en private partijen om in het kader van het tegengaan van terrorismefinanciering samen te werken, duidelijk dat zonder samenwerking terrorismefinanciering niet eenvoudig te detecteren en te voorkomen is.

De hierboven beschreven samenwerking geldt voor een aantal geselecteerde instellingen en niet voor vele andere Wwft-instellingen. Dit terwijl deze wel aan dezelfde wettelijke vereisten en verwachtingen moeten voldoen als de geselecteerde instellingen. Gezien het succes van samenwerking en informatiedeling, zoals uit het FIU Jaaroverzicht blijkt, zou het verstandig zijn om (steeds) meer instellingen bij deze publiek-private samenwerking te betrekken. Iedereen is ervan overtuigd dat het detecteren en voorkomen van terrorismefinanciering uiterst belangrijk is. Wellicht is het in een dergelijke situatie dan beter om de wortel te gebruiken in plaats van de stok. ■

[27] FATF, *Financing of Recruitment for Terrorist Purposes*, januari 2018, p. 27.

[28] Maud Bökkerink, *Een andere aanpak voor het detecteren en melden van ongebruikelijke en verdachte transacties is broodnodig*, 29 oktober 2017, http://www.riskcompliance.nl/news/een-andere-aanpak-voor-het-detecteren-en-melden-van-ongebruikelijke-en-verdachte-transacties-is-broodnodig/.

Veranderingen in landschap van verzekeringsdistributie bieden verzekeraars en adviseurs kansen om de dienstverlening aan klanten te verbeteren

drs. M.A.M. Arts, mr. A.M.F. de Groot & mr. drs. K. Raaijmakers*

Trefwoorden: Insurance distribution directive, IDD, verzekeren, technologie

Inleiding

De afgelopen jaren hebben onder meer het provisieverbod en technologische ontwikkelingen het bedrijfsmodel van verzekeraars, gevolmachtigd agenten, adviseurs en bemiddelaars (hierna ook wel 'de distributieketen van verzekeringen') ingrijpend veranderd. De komende tijd zullen verschillende ontwikkelingen een beroep blijven doen op het verandervermogen van de partijen in deze distributieketen. Technologische innovatie, vergrijzing, veranderend klantgedrag, uitdagende economische omstandigheden en nieuwe wet- en regelgeving hebben invloed op de vraag hoe verzekeren vorm krijgt en wat nog verzekerbaar is.

In dit artikel concentreren we ons op de vraag hoe veranderend klantgedrag en technologische veranderingen leiden tot veranderingen in de distributieketen van verzekeringen en hoe de komst van nieuwe Europese wetgeving op het gebied van verzekeringsdistributie door deze partijen benut kan worden als kans. We schetsen allereerst de belangrijkste ontwikkelingen in de verzekeringsmarkt en de impact die deze veranderingen hebben op de distributie van verzekeringen. Vervolgens beschrijven we hoe deze ontwikkelingen en de invoering van de Europese richtlijn verzekeringsdistributie (*Insurance distribution directive*, IDD) de sector kansen bieden om product en dienst gerichter te laten aansluiten op de behoeften van de klant. We eindigen met een aantal concrete tips voor compliancemedewerkers in deze tijden van verandering.

Technologische ontwikkelingen veranderen zowel aanbod van als vraag naar verzekeringen[1]

De razendsnelle ontwikkeling van technologische mogelijkheden heeft een impact op de structuur van en wijze van dienstverlening in de financiële sector in het algemeen en de verzekeringssector in het bijzonder. Intensiever en meer geïntegreerd gebruik van data, verregaande automatisering, machine learning, blockchain en open digitale platformen zijn hiervan voorbeelden. Het zorgt onder andere voor nieuwe, gespecialiseerde toetreders, faciliteert nauwkeurigere risico-inschattingen, beïnvloedt het productassortiment en stimuleert nieuwe manieren van klantbenadering en klantgedrag.

* Mark Arts en Anne de Groot zijn beiden werkzaam als senior toezichthouder op de afdeling Verzekeren en Pensioenen bij de Autoriteit Financiële Markten. Karina Raaijmakers is directeur Toezicht en Handhaving van de Nederlandse Zorgautoriteit (NZa). Zij schreef dit artikel als hoofd Toezicht Verzekeren en Pensioenen bij de Autoriteit Financiële Markten (AFM).

[1] Technologische innovatie komt als een belangrijke driver voor verandering in de verzekeringssector naar voren in rapporten als Commissie Verzekeraars (2015), '*Nieuw leven voor verzekeraars*', en DNB (2016), *Visie op de toekomst van de verzekeringssector.*

Technologische ontwikkelingen veranderen niet alleen het aanbod van verzekeringen, maar ook de vraag naar verzekeringen. Nederlandse consumenten gebruiken technologische (hulp) middelen volop. Het internet geeft consumenten de mogelijkheid om 24 uur per dag op de hoogte te blijven van het laatste nieuws en aanbiedingen via online bronnen. Nederland is koploper op gebied van technologiegebruik in Europa: 80 procent van de Nederlanders bankiert online, aankopen via internet groeien van jaar op jaar en 70 procent bezit basisvaardigheden op ICT-gebied.[2] Dit maakt dat Nederlandse consumenten het steeds meer gewoon gaan vinden (geld)zaken via internet te doen. Dit geldt ook voor het afsluiten en aanpassen van verzekeringen en het melden en afhandelen van schades.

Daarnaast leidt het toenemend gebruik van internet door de consument ertoe dat er steeds data beschikbaar is over de consument. Dit betekent dat consumenten die online actief zijn meer de mogelijkheid krijgen om te 'shoppen' met hun profielen en zelf de gegevens over hun levensstijl en voorkeuren te gelde te maken. Deze trend creëert naar verwachting ruimte voor een markt waarin consumenten hun behoeftes en wensen kunnen 'vermarketen'. In het geval dat de klant zelf baas over eigen data wordt, moeten partijen die data over hun klanten verzamelen in ruil daarvoor een duidelijke toegevoegde waarde bieden. Dit zal op termijn vermoedelijk leiden tot een steeds betere match tussen vraag en aanbod van verzekeringsproducten.[3]

Toekomstbeeld voor de komende jaren: consumenten regelen de meeste schadeverzekeringen zelf online.
Doorontwikkelde apps geven consumenten inzicht en de mogelijkheid om aanpassingen op elk moment door te voeren. Miniverzekeringen worden doorlopend afgesloten: de consument maakt foto's van het interieur en binnen het kwartier is de nieuwe polis met een verhoogde verzekerwaarde ontvangen. Een consument sluit een reisverzekering voor een specifieke vlucht, terwijl hij in de rij voor de douane staat.

Bij veel schadeverzekeringen is de kern van producten hetzelfde, maar de wijze waarop de producten online worden aangeboden is gepersonaliseerd. De meerderheid van klanten zijn bereid om hun datagegevens te delen met aanbieders in ruil voor lagere premies. De loyaliteit met specifieke verzekeringsmerken is verder afgenomen en klanten stappen vaak over naar andere aanbieders. Daarnaast is de behoefte van zelfstandige ondernemers en flexwerkers om inkomensverlies en aansprakelijkheid af te dekken toegenomen.

Tegenover de mogelijkheden die technologie en data consumenten bieden, staat dat in de afgelopen jaren steeds meer focus op privacy en een groeiende zorg over het klakkeloos delen van data is ontstaan, de zogenaamde privacy paradox. Ook financiële instellingen zullen hun klantdata proberen te gelde te maken. Bovendien kan een betere risico-inschatting op basis van data door de verzekeraar leiden tot een steeds meer gepersonaliseerde premiestelling, wat de premies voor consumenten met een hoog risicoprofiel mogelijk onbetaalbaar maakt.[4] Hierdoor kan de facto uitsluiting van bepaalde groepen consumenten ontstaan.

Ook maatschappelijke en politieke ontwikkelingen hebben invloed op klantgedrag en daarmee op verzekeringsdistributie

Niet alleen technologische ontwikkelingen hebben invloed op het klantgedrag. Er zijn verschillende maatschappelijke en politieke ontwikkelingen die invloed hebben op het gedrag van klanten ten opzichte van verzekeringen. Dit uit zich vooral in een verschuiving van het collectief naar het individu.

1. **Individuele keuzes en belangen staan nadrukkelijker centraal voor consumenten**.
   Consumenten verlangen steeds meer maatwerk en keuzevrijheid. Dit kan de kenmerken van een verzekeringsproduct beïnvloeden, maar beïnvloedt ook de wijze waarop de verzekering wordt aangeboden. Consumenten willen op een persoonlijke manier benaderd en geholpen worden. Zij worden geconfronteerd met nieuwe mogelijkheden op het gebied van verzekeringen en ontwikkelen tegelijkertijd nieuwe wensen en behoeftes. Mensen staan

[2] CBS (2016), *ICT-vaardigheden van Nederlanders.*
[3] Reaal (2015), *Trends & Ontwikkelingen 2016-2018: Macrotrends, consumententrends, distributieontwikkelingen en financiële markt*.
[4] DNB (2016), *Visie op de toekomst van de verzekeringssector' en Verbond van Verzekeraars (2015), 'Gebruik van persoonlijke gegevens in verzekeringskosten.*

steeds meer zelf aan het roer en zijn mondiger: ze stellen meer eisen, eisen hun rechten op en zijn eerder geneigd anderen op hun vermeende verantwoordelijkheid aan te spreken. Deze beweging vertaalt zich in twee ontwikkelingen:

a. Verzekeren lijkt door consumenten steeds meer als een te calculeren recht op een vergoeding te worden beschouwd, zoals te zien bij aanvullende zorgverzekeringen, in plaats van deling van een onvoorzien risico. Dit lijkt een fundamentele aantasting van het traditionele verzekeringsprincipe te vormen en leidt tot een toename in claimgedrag.
b. Er ontstaat een grotere behoefte aan maatwerk en het personaliseren van producten en diensten.5 Consumenten (deels) willen en kunnen meer (financiële) zaken zelf regelen, omdat het makkelijker wordt om dit zelf te doen en omdat voor advies betaald moet worden. Klanten willen meer doen en dat geldt vooral voor de eenvoudige (af te sluiten) producten en diensten. Bij complexere vraagstukken lijkt persoonlijke dienstverlening echter onverminderd belangrijk.[6]

2. **De solidariteit onder consumenten verschuift van het collectief naar de eigen groep**. Van het individu wordt meer flexibiliteit en zelfredzaamheid verwacht. Tegelijkertijd ontlenen mensen hun identiteit en daarmee hun bestaan in mindere mate aan traditionele sociale groepen (op basis van geloof, politieke overtuiging, sociale klasse etc.), maar zoeken juist naar nieuwe sociale verbanden en nieuwe collectiviteiten.[7] Consumenten willen graag zaken doen met mensen die ze vertrouwen en dit genereert de opkomst van nieuwe deelmarkten. Solidariteit is een belangrijk fundament onder publieke voorzieningen en verzekeringen en het klassieke model van brede risico-pooling lijkt daardoor onder toenemende druk te staan.
3. **Het toenemende individualisme gaat gepaard met toenemende individuele verantwoordelijkheid**. Consumenten moeten meer eigen verantwoordelijkheid nemen voor hun geldzaken zoals pensioen en zorg, en dit geldt ook voor het afdekken van risico's in de bredere zin (verzekeren). Dit geldt in bijzonder voor specifieke groepen consumenten. De groep zelfstandigen zonder personeel (zzp) in Nederland is sterk toegenomen in de afgelopen 10 jaren en is groot in vergelijking met andere landen.8 Hetzelfde geldt voor de groep mensen in dienst met flexibele arbeidsvoorwaarden. Deze groeiende groep consumenten draagt meer verantwoordelijkheid dan voorheen. De complexiteit bij financiële besluiten en het beperkte vermogen van consumenten om risico's op een objectieve manier in te schatten is echter niet veranderd. Keuzestress en inertie blijven onveranderlijk aanwezig.

Veranderingen hebben effect op de verzekeringsdistributie

Rolverdeling tussen aanbieders en het intermediair

Integrale dienstverlening bij aanbieders van financiële producten en het feit dat consumenten meer zelf kunnen regelen, zorgen voor een veranderende rolverdeling tussen de verzekeraar en het intermediair. Het intermediair krimpt en verandert van samenstelling. Het provisieverbod en de directe online verkoop dwingen adviseurs en bemiddelaars tot een verdienmodel dat kwetsbaarder is voor veranderende economische omstandigheden. Consumenten zijn door technologische ontwikkelingen steeds beter in staat meer zelf te doen. Hierdoor neemt het aanbod van online verkoop, met of zonder advies, toe.[9] De opkomst van vergelijkingssites faciliteert deze ontwikkeling.[10] Lagere marges, onder meer door de komst van nieuwkomers, leiden naar verwachting tot steeds meer online-oplossingen, zoals robo-advies.

Rol van volmachtbedrijven en serviceproviders

Volmachtbedrijven en serviceproviders zijn nog belangrijke tussenschakels tussen verzekeraar en intermediair. Bij de distributie van met name schadeverzekeringen spelen volmachtbedrijven en serviceproviders op dit moment nog een belangrijke rol als tussenschakel tussen enerzijds de verzekeraars en anderzijds de adviseurs en bemiddelaars. Technologische innovaties, het veranderende klantgedrag en wet- en regelgeving gaan naar verwachting effect hebben op de toekomst van het volmachtbedrijf. Enerzijds blijven de redenen voor uitbesteding aan gevolmachtigd agenten bestaan:

5 TNO (2013), *Oog voor innovatie.*
6 Reaal (2015), *Trends & Ontwikkelingen 2016-2018: Macrotrends, consumententrends, distributieontwikkelingen en financiële markt*.
7 TNO (2013), *Oog voor innovatie.*
8 Interdepartementaal Beleidsonderzoek (2015), *Zelfstandigen zonder personeel.*
9 Verbond van verzekeraars (2015), *Verzekerd van cijfers.*
10 DNB (2016), *Visie op de toekomst van de verzekeringssector.*

schaalvoordelen, distributiekracht en kostenbeheersing bij verzekeraars. Anderzijds zullen de verscherpte normen op grond van Europese regelgeving als Solvency II op de risicobeheersing van de uitbestedingsrelatie mogelijk leiden tot afname van de rol van volmachtbedrijven in de distributie van schadeverzekeringen.

Van entity-based naar activity-based verzekeringen

Er lijkt een verschuiving van *entity-based* naar *activity-based* verzekeringen op te treden. Waar van oudsher verzekeringen een duidelijk financieel product zijn die je via een verzekeraar of financieel adviseur afsluit, vormen verzekeringen vandaag de dag steeds vaker een onderdeel van de aankoop van consumentengoederen. Zo zijn autoverzekeringen steeds vaker een onderdeel van private lease contracten en bij zelfsturende auto's verschuift dit wellicht zelfs naar de fabrikant. Ook bij de aankoop van telefoons, koelkasten en wasmachines (feitelijk een verlenging van de wettelijke garantieplicht) en vluchten (reisverzekeringen) worden schadeverzekeringen verkocht. Verzekeringen zijn daarmee steeds meer een productkenmerk en worden daarmee makkelijk mee afgesloten bij een aankoop. Hierdoor verandert het kanaal, via welke verzekeringen worden verkocht, steeds ingrijpender: niet enkel partijen wiens *core business* het is om financiële producten te adviseren en te sluiten, maar grote winkelketens voor consumentengoederen vervullen een belangrijke rol in het landschap van verzekeringsdistributie.

Verzekeraars schuiven op in de waardeketen

Verzekeraars breiden hun diensten uit en concurreren op nieuwe plekken in de waardeketen. Bij sommige verzekeraars is een verschuiving van de aandacht van overname van verzekeringstechnische risico's naar dienstverlening tegen vergoeding (van premie- naar 'fee-based') waarneembaar.[11] Advisering en preventie worden bijvoorbeeld een belangrijker werkterrein. Ook bieden verzekeraars vaker integrale financiële planning voor particulieren en kleine ondernemers aan in plaats van losse producten, zoals lijfrentes of overlijdensrisicoverzekeringen. Verzekeraars concurreren bij individuele vermogensopbouw, collectief leven en kredietverlening direct met banken, pensioenfondsen[12] en andere financiële dienstverleners (zoals vermogensbeheerders).[13] Andersom concurreren deze entiteiten ook steeds directer met verzekeraars. Zo hebben bankspaarproducten eerder al de markt van individuele levensverzekeringen grotendeels overgenomen en vormen het Algemeen Pensioenfonds en de Premiepensioeninstelling nieuwe concurrentie voor de traditionele pensioenverzekeraar. Kortom de grenzen tussen sectoren komen daarmee verder te vervagen.

InsurTech

Nieuwe fintechpartijen (in de context van verzekeren ook wel 'InsurTech bedrijven' genoemd) en nieuwe concepten vinden hun weg naar de verzekeringsmarkt. InsurTech bedrijven proberen met de inzet van nieuwe technologieën een specifieke positie in de waardeketen in te nemen, vooral in de schademarkt. Deze partijen hebben een tijdelijke voorsprong op gevestigde verzekeraars, die minder snel kunnen innoveren. In opkomst zijn nieuwe concepten als 'on-demand'-verzekeringen[14] en portefeuillebeheer. Cruciaal bij deze technologische ontwikkelingen is het eigendom van de verzamelde data en het recht om deze te gebruiken voor het ontwikkelen en beheren van verzekeringsproducten. Verder zijn er steeds meer initiatieven op het gebied van 'peer-to-peer'-verzekeren, waarbij een klein netwerk een schadeverzekeringspool vormt. Ook wordt hierbij vaak gebruik gemaakt van de teruggeefformule: als weinig of geen claims plaatsvinden, krijgen de deelnemers een deel van de ingelegde premie terug. In Nederland zijn er al een aantal voorbeelden van InsurTech bedrijven (bijvoorbeeld OurSurance[15] en Fairzekering[16])[17], terwijl in bijvoorbeeld Duitsland en de Verenigde Staten de

[11] In de markt is overigens ook een tegengestelde beweging te zien. Verzekeraars die zich vooral concentreren op het verzekeren van het risico en bijvoorbeeld de schadeafhandeling buiten de deur zetten.

[12] Denk ook aan de oprichting van APF's door verzekeraars.

[13] DNB (2016), *Visie op de toekomst van de verzekeringssector.*

[14] Voorbeeld hiervan is Gappie van NN; een app waarmee je 'on demand' per uur een verzekering voor een geleende auto verzekert en betaalt.

[15] Een platform dat op basis van blockchain technologie en 'smart contracts' klanten en investeerders bij elkaar wil brengen (p2p verzekeringen) en verzekeringen wil automatiseren.

[16] Zie AMWeb (30 juni 2016): 'Waar blijven de Nederlandse investeringen in InsurTech?'.

[17] Daarnaast zijn meerdere partijen, zoals de ANWB, bezig met het kastje in de auto. Dit genereert voor de verzekeraar zowel data over gedrag als dat het mogelijk maakt de pricing op het gedrag af te stellen.

ontwikkeling al verder is. Denk aan FriendSurance, Lemonade en Oscar[18] en verzekeringsplatform Trov.

Europese richtlijn IDD speelt met kanaalneutrale wetgeving in op de veranderende verzekeringsdistributie

Op 1 juli 2018 moet in alle Europese landen de richtlijn verzekeringsdistributie (de IDD) zijn geïmplementeerd. De IDD zal dan de richtlijn verzekeringsbemiddeling uit 2002 vervangen, die al in onze Wet op het financieel toezicht (Wft) is geïmplementeerd. De Nederlandse wetgever ligt op schema met de implementatie van de IDD in de Wft en de daaronder hangende lagere regelgeving, en Nederland zal de Europese implementatie-deadline dan naar verwachting ook halen.

De IDD behoort tot hetzelfde pakket aan maatregelen als de *Markets in Financial Instruments Directive and Regulation* (MiFID II/MiFIR) en de *Mortgage Credit Directive* (MCD), dat moet leiden tot een eenduidig en uitvoerbaar pakket aan Europese regelgeving op het gebied van consumentenbescherming. Met de IDD heeft de Europese wetgever geprobeerd zoveel mogelijk in te spelen op de veranderende markt van verzekeringsdistributie, door onder meer technologische ontwikkelingen en veranderend klantgedrag. Zo is het eerste hoofddoel van de IDD het creëren van een gelijk speelveld voor alle marktpartijen die bij de distributie van verzekeringen zijn betrokken (intermediaire aanbieders, directe aanbieders, onafhankelijke adviseurs, bemiddelaars, vergelijkingssites).

Hiervoor werd al beschreven dat verzekeringen steeds vaker een onderdeel vormen van de aankoop van consumentengoederen. De IDD speelt in op deze ontwikkeling door een meer gelijk speelveld te creëren tussen het traditionele intermediair en partijen die bemiddelen in verzekeringen als nevendienst, zoals reisbureaus en autoverhuurbedrijven. De IDD beperkt de vrijstellingsmogelijkheden voor deze partijen van de vergunningsplicht waardoor veel van deze partijen de normen van de Wft moeten naleven. Concreet zullen met de inwerkingtreding van de IDD partijen die verzekeringen afsluiten in aanvulling op een goed of dienst onder de reikwijdte van de wetgeving komen te vallen tenzij zij verzekeringen distribueren met een jaarpremie van minder dan 600 euro per jaar (pro rata berekend), of tenzij bij verzekeringen die korter lopen dan drie maanden, de nominale premie minder dan 200 euro bedraagt.

Tweede hoofddoel van de IDD is het verbeteren van de bescherming van de consument. Vanwege het veranderend klantgedrag en de effecten daarvan op de distributie van verzekeringen mag er volgens de Europese wetgever geen verschil zijn in consumentenbescherming tussen de verschillende kanalen waar een consument zijn verzekering kan afsluiten. Of de consument nu kiest om bij een adviseur op de hoek naar binnen te lopen, of zijn verzekering online sluit, behoort voor bescherming van de consument niet uit te maken. Met andere woorden: consumentenbescherming moet 'kanaalneutraal' zijn. Om deze reden zijn er in de IDD aanpassingen gedaan in de wettelijke definitie van het begrip bemiddelen in art. 1:1 Wft, waardoor de toepassing van deze definitie in een online omgeving wordt verduidelijkt. Na invoering van de IDD in de Nederlandse Wet op het financieel toezicht (Wft) ligt vast dat er ook sprake kan zijn van bemiddelen als de vergelijkingssite relevante klantinformatie inwint en mede op basis hiervan een vergelijking maakt. De klant kan via de vergelijkingssite (via bijvoorbeeld een link) terecht komen bij de aanbieder of bij een andere bemiddelaar, waar hij opnieuw zijn gegevens invoert. Deze werkwijze valt onder de definitie van bemiddelen als de vergelijkingssite een contract heeft met de aanbieder of een andere bemiddelaar dat tot doel heeft om de aanbieder of bemiddelaar met consumenten in contact te brengen om een overeenkomst tot stand te laten komen. Bij deze werkzaamheden is er immers geen sprake van het enkel doorverwijzen van de klant door de vergelijkingssite.[19]

IDD als kans om product en dienstverlening gerichter te laten aansluiten op de behoefte van de klant

De IDD biedt volgens ons een kans voor Nederlandse verzekeraars en adviseurs om de sprong naar een innovatieve en technologisch vooruitstrevende toekomst te maken, en ervoor te zorgen dat hun product terecht komt bij de juiste klant, ongeacht via welk kanaal de klant de verzekering afsluit.

[18] Zie o.a. AMWeb (10 januari 2017): '*InsurTech stapt uit de schaduw van FinTech*'.

[19] Zie: https://www.rijksoverheid.nl/documenten/kamerstukken/2017/09/06/nader-rapport-wetsvoorstel-implementatie-richtlijn-verzekeringsdistributie.

De IDD is er namelijk voor een belangrijk deel op gericht om het verzekeringsproduct zo goed mogelijk te laten aansluiten op de wensen en behoeften van de klant. Of deze nu afsluiten bij een verzekeraar, een adviseur of een vergelijkingssite. Met of zonder advies. Zo introduceert de IDD de normen omtrent het laten aansluiten van het product bij de wensen en behoeften van de specifieke klant. Deze normen zijn in Nederland geïmplementeerd in art. 4:22a Wft. Deze normen brengen mee dat de informatie die de verzekeraar, adviseur of ieder ander met klantcontact verstrekt moet aansluiten op de door de klant zelf kenbaar gemaakte wensen en behoeften. Met andere woorden: als de klant zelf kenbaar maakt op zoek te gaan naar een verzekering met bepaalde dekking, dan moet de informatie over verzekeringen die vervolgens wordt verstrekt aansluiten bij deze behoefte van de klant. Dit geldt voor zowel situaties waarin wordt geadviseerd als *execution only* situaties.

Ook de nieuwe productontwikkelingsnormen uit de IDD zijn erop gericht het juiste product bij de juiste doelgroep te krijgen. Verzekeraars en adviseurs zullen er samen voor De nieuwe productontwikkelingsnormen uit de IDD gelden voor verzekeraars, adviseurs, bemiddelaars en gevolmachtigd agenten. Verzekeraars en gevolmachtigd agenten hebben al sinds 2013 te maken met productontwikkelingsnormen, maar voor de meeste adviseurs en bemiddelaars zijn ze helemaal nieuw. De productontwikkelingsnormen worden in Nederland geïmplementeerd in art. 32 en 32e BGfo Wft en zullen volgen uit de rechtstreeks werkende Europese Uitvoeringsverordening.[20]

De IDD brengt mee dat aanbieders vooraf moeten bepalen voor welke doelgroep het financiële product bestemd is, waarbij de behoeften, kenmerken en doelstellingen in kaart worden gebracht. Ook stelt de aanbieder bij voorkeur vast voor welke groep van consumenten het product niet bedoeld is. Alle partijen in de distributieketen, waaronder adviseurs, vergelijkingssites en aanbieders, moeten zich inspannen om ervoor te zorgen dat financiële producten terechtkomen bij de consumenten voor wie het product is ontwikkeld. Zo moet de aanbieder per verzekeringsproduct de geschikte distributiestrategie bepalen. Om te zorgen dat het verzekeringsproduct wordt gedistribueerd aan de juiste doelgroep moet de aanbieder distributeurs informeren over de kenmerken van het product, het productontwikkelingsproces, de doelgroep en de distributiestrategie. Deze informatie stelt de distributeur in staat om het verzekeringsproduct aan de juiste doelgroep te distribueren. De aanbieder moet het product testen aan de hand van scenario-analyses en periodiek evalueren of het product nog voldoet. De verzekeringsdistributeur moet ervoor zorgen dat zijn distributiestrategie en doelgroep in lijn is met die van de aanbieder en hij moet zijn distributieproces periodiek evalueren, waarbij hij moet verifiëren of verzekeringsproducten zijn verkocht aan de geïdentificeerde doelgroep.

Tot slot zal ook de aanscherping van de vereisten over productinformatie de kans vergroten dat verzekeringsproducten bij de juiste consumenten terechtkomen. Uitgangspunt van de IDD is dat de consument gelijke informatie over de dienstverlening en het verzekeringsproduct moet ontvangen, ongeacht via welk kanaal hij het product afsluit. Dus of de consument nu bij een fysieke adviseur zijn product afsluit of online zonder advies, na invoering van de IDD zal de consument het nieuwe standaarddocument over schadeverzekeringen (*Insurance product information document,* ofwel: IPID) ontvangen. In Nederland wordt de plicht om het IPUD te verstreken neergelegd in art. 49a BGfo Wft. Het IPID moet verstrekt worden voorafgaand aan het sluiten van alle schadeverzekeringen, waaronder zorgverzekeringen. In het IPID is in een oogopslag de meest essentiële informatie over het verzekeringsproduct te vinden voor de consument. Denk aan: de verzekeringsdekking, de wijze en duur van betaling van premies, belangrijkste uitsluitingen en verplichtingen die uit de overeenkomst voortvloeien, de looptijd en wijze van beëindiging van de overeenkomst. Het format waaraan het IPID moet voldoen is in elk Europees land gelijk: dit volgt namelijk uit een rechtstreeks werkende Uitvoeringsverordening.[21]

Afsluiting

We zijn in dit artikel in vogelvlucht door de veranderende wereld van verzekeringsdistributie gegaan. We sluiten graag af met enkele concrete checks die compliance professionals in de financiële sector kunnen uitvoeren om te controleren of de onderneming waarvoor zij werkzaam zijn nog een eindsprint moet inzetten om per 1 oktober 2018 te voldoen aan de IDD.

[20] http://ec.europa.eu/finance/docs/level-2-measures/idd-delegated-regulation-2017-6218_en.pdf.

[21] (EU) 2017/1469. Zie hier: http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32017R1469&rid=8.

1. Vallen de werkzaamheden die mijn onderneming verricht onder de aangepaste definitie van bemiddelen in de Wet op het financieel toezicht (zie hierboven)? Zo ja, moet mijn onderneming een vergunning aanvragen?
2. Is mijn onderneming voldoende transparant voorafgaand aan de dienstverlening aan de consument? Informeert mijn onderneming de consument over de wijze van beloning, eigendomsverhoudingen en wijze van adviseren?
3. Voldoen de samenwerkende bemiddelaars aan de voorwaarden van de vrijstelling onder de IDD? Zo nee, moeten zij een vergunning aanvragen?
4. Voldoet het huidige productontwikkelingsproces aan de normen die de IDD daaraan stelt? Is er voor elk verzekeringsproduct een distributiestrategie opgesteld en een doelgroep geïdentificeerd? Is tevens beschreven voor welke consumenten het verzekeringsproduct niet geschikt is?
5. Dient mijn onderneming het standaardinformatiedocument voor schadeverzekeringen aan te maken en/ of te verstrekken aan de consument? ■

FinTech & Wwft

Innovatie in het klantacceptatieproces: waarborgen en aandachtspunten

mr. T.W.G. de Wit*

Trefwoorden: innovatie, fintech-oplossingen, klantacceptatieproces

Innovatie in het klantacceptatieproces

Financiële dienstverlening is de laatste jaren in rap tempo gedigitaliseerd. Klanten worden tegenwoordig veelal online of mobiel bediend en zij verwachten snelle, goedkope en persoonlijke dienstverlening. Om aan die wensen te kunnen voldoen moeten marktpartijen onderling concurreren en innoveren. Met name ten aanzien van de inrichting van het klantacceptatieproces leidt dit niet zelden tot hoofdbrekens. Enerzijds moeten marktpartijen het klantacceptatieproces zo kostenefficiënt mogelijk inrichten en mag de klantacceptatie niet afdoen aan de beleving van de klant en snelheid waarmee deze bediend kan worden. Anderzijds brengt de digitale dienstverlening vanwege het gebrek aan fysiek contact juist nieuwe en verhoogde risico's en uitdagingen met zich mee voor de inrichting van het klantacceptatieproces. Dit stelt marktpartijen (hierna: 'Wwft-instellingen') voor een lastige uitdaging: de business faciliteren op een manier waarop naleving van de Wet ter voorkoming van witwassen en financieren van terrorisme ('Wwft') en de Sanctiewet 1977 voldoende is gewaarborgd. Dit is het moment waar innovatieve oplossingen voor het klantacceptatieproces om de hoek komen kijken en uitkomst kunnen bieden.

In dit artikel ga ik in op de mogelijkheden om dergelijke innovatieve oplossingen voor het klantacceptatieproces in te zetten voor een (kosten)efficiëntere naleving van de Wwft (hierna: 'FinTech-oplossing') en de aandachtspunten die daarbij gelden. Met FinTech-oplossing doel ik dan op een innovatieve tool of applicatie die een marktpartij kan integreren in het klantacceptatieproces of de transactiemonitoring, vaak om naleving van de Wwft (kosten)efficiënter in te richten en de klantbeleving te verhogen. Ik bespreek de aandachtspunten aan de hand van een recente opinie van de European Supervisory Authorities[1] ('ESA's').

* Tim de Wit is advocaat bij Finnius in Amsterdam.

[1] De ESA's bestaan uit de European Banking Authority ('EBA'), de European Insurance and Occupational Pensions Authority ('EIOPA') en de European Securities and Markets Authority ('ESMA').

[2] JC 2017 81, 23 January 2018, Opinion on the use of innovative solutions by credit institutions and financial institutions in the customer due diligence process.

[3] Richtlijn (EU) 2015/849.

Recent hebben de ESA's zich voor het eerst uitgesproken over de mogelijkheden om FinTech-oplossingen te integreren in het klantacceptatieproces en de daarbij te treffen maatregelen

De Opinie

Recent hebben de ESA's zich voor het eerst uitgesproken over de mogelijkheden om FinTech-oplossingen te integreren in het klantacceptatieproces en de daarbij te treffen maatregelen. Het standpunt van de ESA's is neergelegd in een opinie: '*Opinion on the use of innovative solutions by credit institutions and financial institutions in the customer due diligence process*'[2] (de 'Opinie'). Zoals zal blijken is de Opinie niet alleen relevant bij de beoordeling van de specifieke kenmerken van een FinTech-oplossing, maar biedt deze ook een interessante inkijk in het niveau van maatregelen die de ESA's van marktpartijen verwachten voor naleving van de Wwft. De maatregelen reiken verder dan alleen het beoordelen van een FinTech-oplossing, maar raken ook de hele inrichting van de bedrijfsvoering en governance rond naleving van de Wwft. Bij nadere bestudering blijken hier ook zeer interessante overwegingen in te staan die ook zonder het gebruik van een FinTech-oplossing relevant zijn voor de inrichting van het klantacceptatieproces. Hieronder ga ik nader in op de Opinie en de door de ESA's geformuleerde maatregelen.

Reikwijdte van de Opinie

De Opinie is geadresseerd aan de toezichthouders die bevoegd zijn toezicht te houden op naleving van de nationale implementatie van de Vierde Anti-witwasrichtlijn[3] ('AMLD4') (in Nederland zijn dit De Nederlandsche Bank ('DNB') en de Autoriteit Financiële Markten ('AFM')). Wwft-instellingen die FinTech-oplossingen willen integreren in hun klantacceptatieproces doen er dus goed aan deze Opinie te raadplegen, omdat hierin het toetsingskader voor DNB en de AFM is vastgelegd.

In Nederland is AMLD4 overigens nog niet geïmplementeerd. De verwachting is dat dit in de loop van 2018 zal gebeuren. AMLD4 wordt geïmplementeerd in

de Wwft[4] en het Uitvoeringsbesluit Wwft 2018.[5] De Opinie is dus relevant voor uitleg van de verplichtingen uit hoofde van AMLD4, die in Nederland nog niet gelden. Niettemin is naar mijn mening deze Opinie ook nu al relevant voor de uitleg van de verplichtingen uit hoofde van de huidige Wwft (die overigens primair gebaseerd is op de voorganger van AMLD4, de Derde Anti-witwasrichtlijn[6] ('AMLD3')).

In de Opinie geven de ESA's de factoren mee die de AFM en DNB zouden moeten meewegen

In de Opinie geven de ESA's de factoren mee die de AFM en DNB zouden moeten meewegen wanneer: (i) zij de effectiviteit van de klantacceptatieprocessen toetsen waarin Wwft-instellingen FinTech-oplossingen hebben geïntegreerd en (ii) zij de controlemechanismen beoordelen aan de hand waarvan Wwft-instellingen de risico's mitigeren die gepaard gaan met de FinTech-oplossing(en).

Type innovatieve oplossingen

De ESA's constateren dat Wwft-instellingen zich bij de keuze voor bepaalde FinTech-oplossingen met name laten leiden door een verbeterde klantbeleving en kostenbesparingen. De meeste oplossingen zijn dus hierop gericht. Grofweg zien de ESA's twee type FinTech-oplossingen die momenteel gebruikt worden:

1. Oplossingen die voorzien in niet-fysieke verificatie van de identiteit van de klant op basis van diens traditionele identiteitsdocumenten (zoals een paspoort of rijbewijs) met behulp van bijvoorbeeld een *smartphone*.
2. Oplossingen die voorzien in verificatie van de identiteit van de klant op een andere manier, zoals via een centrale bewaarplaats van identiteitsdocumenten (*central identity documentation repository*). Zo'n centrale bewaarplaats is dan veelal een samenwerking van verschillende marktpartijen die binnen het bereik van AMLD4 vallen. Het doel van zo'n bewaarplaats is dat informatie maar één keer hoeft te worden opgevraagd en daarna kan worden gedeeld met de deelnemers van de bewaarplaats.

Er zijn inderdaad verschillende initiatieven op dit vlak waarneembaar. Bepaalde dienstverleners voorzien in de behoefte om alleen de verificatie van de identiteit op afstand te faciliteren, door daar bijvoorbeeld een tool voor te ontwikkelen (i) voor de smartphone waarbij de klant een foto van zijn of haar identiteitsbewijs kan maken of (ii) die live videochats of videoconferences mogelijk maken met de klant.[7] Andere dienstverleners richten zich juist op het vergemakkelijken van het hele klantacceptatieproces, door een tool te ontwikkelen waarbij de klant in een online of mobiele applicatie al zijn of haar verplichte gegevens en documentatie kan invoeren.

De ESA's zien ook een toenemend gebruik van FinTech-oplossingen om de relatie met de klant en diens transacties te monitoren. Dat soort oplossingen werken dan veelal op basis van *artificial intelligence* en bepaalde algoritmen, die de Wwf-instellingen in staat stellen om grote hoeveelheden data van verschillende bronnen te verwerken. De FinTech-oplossing blijft zichzelf continue verbeteren aan de hand van data uit het verleden en als de oplossing goed is geïntegreerd, kan deze bijdragen aan:

- Het monitoren van risico's die verbonden zijn aan een klant of bepaalde transacties, door zowel interne informatie (zoals rekeningdetails en verrichte transacties) als externe informatie (zoals UBO-registers, bepaalde media of Google en PEP-lijsten) mee te wegen (waaronder bijvoorbeeld ook in verschillende talen).
- Het verder automatiseren van monitoringsystemen, zodat de capaciteit en inzet van medewerkers van de Wwft-instelling uit kan gaan naar analyse van de data.
- Een verbeterde besluitvorming ten aanzien van mogelijke ongebruikelijke transacties door het ontvangen van *instant alerts*.
- Het beperken van foutieve informatie of meldingen.

Zo bezien kunnen FinTech-oplossingen dus niet alleen een positieve bijdrage leveren aan de klantbeleving en kostenbesparing, maar kunnen zij ook daadwerkelijk de klantacceptatieprocessen verbeteren

Zorgvuldige afweging

Zo bezien kunnen FinTech-oplossingen dus niet alleen een positieve bijdrage leveren aan de klantbeleving en kostenbesparing, maar kunnen zij ook daadwerkelijk

---

[4] Op het moment van schrijven van dit artikel is het wetsvoorstel inmiddels aangenomen door de Tweede Kamer (op 6 maart 2018). Het wetsvoorstel ligt nu bij de Eerste Kamer.

[5] Het Uitvoeringsbesluit Wwft 2018 is ter consultatie aan de markt voorgelegd op 31 januari 2018. Marktpartijen konden reageren tot en met 28 februari 2018. Het is nu wachten op het definitieve besluit. Het concept Uitvoeringsbesluit Wwft 2018 dat ter consultatie is voorgelegd is te raadplegen via: https://www.internetconsultatie.nl/uitvoeringsbesluitwwft2018.

[6] Richtlijn 2005/60/EG.

[7] Na een snelle rondgang op Google komen partijen voorbij als IDology, Gemalto en Jumio.

de klantacceptatieprocessen verbeteren. Wwft-instellingen mogen wat de ESA's betreft echter niet over één nacht ijs gaan bij de keuze van een FinTech-oplossing en de integratie daarvan. Sterker nog, de ESA's verwachten dat marktpartijen zeer zorgvuldig afwegen, met het oog op de risico's van hun onderneming en de risico's bij individuele klantrelaties, of de implementatie van FinTech-oplossingen wel effectief is. Daarbij moet door de Wwft-instellingen met name gekeken worden naar:

— toezicht en controlemechanismen;
— de kwaliteit en effectiviteit van klantacceptatieprocessen;
— de betrouwbaarheid en afhankelijkheid van klantacceptatieprocessen;
— risico's vanwege het leveringskanaal; en
— geografische risico's.

Hieronder ga ik nader in op deze individuele factoren. Deze af te wegen factoren gelden overigens in aanvulling op de 'algemene' risicofactoren die marktpartijen al moeten afwegen uit hoofde van art. 8 AMLD4 en de zogenoemde *Risk Factor Guidelines*[8] en die verband houden met hun cliënten, landen of geografische gebieden, producten, diensten, transacties en leveringskanalen.

In algemene zin merken de ESA's op dat Wwft-instellingen die FinTech-oplossingen willen integreren, zich een volledig beeld moeten vormen van kenmerken van de oplossing om daarmee voldoende zekerheid te hebben dat de oplossing adequaat werkt en om voorbereid te zijn voor een moment waarop de oplossing (tijdelijk) niet werkt. Wwft-instellingen moeten voldoende in-house kennis en expertise hebben om effectieve integratie en gebruik ervan te waarborgen en om in geval van falen de continuïteit van de klantacceptatieprocedures te waarborgen. Uiteindelijk moet natuurlijk worden voorkomen dat – vanwege een falen van het systeem – klanten worden geaccepteerd die normaliter niet door het klantacceptatieproces zouden komen. Dit gaat vrij ver en betekent volgens de ESA's in ieder geval dat Wwft-instellingen zichzelf moeten afvragen:

— Of er voldoende technische kennis aanwezig is om de implementatie van de FinTech-oplossing te overzien, met name wanneer deze zijn ontwikkeld of worden uitgevoerd door derde partijen?
— Of de leiding en de compliance officer voldoende begrip hebben van de FinTech-oplossing?
— Of er een gedegen calamiteitenplan aanwezig is in geval van falen van de FinTech-oplossing?

Dit is al meteen een zware verplichting voor Wwft-instellingen die FinTech-oplossingen willen integreren in hun klantacceptatieproces. Zeker voor kleinere marktpartijen, voor wie het omwille van kosten en compliance juist nuttig kan zijn FinTech-oplossingen te implementeren, zal het lastig zijn om aan deze eisen van de ESA's te voldoen. Dit zal alleen al zo zijn omdat de keuze voor de oplossing er juist in gelegen zal zijn dat men intern niet voldoende technische of personele middelen heeft. Hier ligt in ieder geval een uitdaging voor de directie van de Wwft-instelling; zij zal moeten vaststellen dat waar de instelling besluit tot implementatie van een FinTech-oplossing, de instelling ook in staat is om de impact daarvan te overzien. Ik kan me voorstellen dat de compliance officer betrokken wordt in deze afweging en daarin een belangrijke rol vervult.

Toezicht en controlemechanismen bij selectie van FinTech-oplossing

Wanneer Wwft-instellingen besluiten FinTech-oplossingen te integreren in hun klantacceptatieproces, moeten zij richting DNB of de AFM kunnen aantonen dat ze adequate governance en controlemechanismen hanteren omtrent besluitvorming voor een FinTech-oplossing in het klantacceptatieproces. DNB en de AFM moeten hierbij de volgende aspecten toetsen:

a. De Wwft-instelling moet de FinTech-oplossing eerst goed en grondig testen voor implementatie. De oplossing moet aansluiten bij het klantacceptatieproces van de Wwft-instelling en moet voldoen aan de relevante wet- en regelgeving. Wanneer de resultaten niet eenduidig zijn, moet de Wwft-instelling de FinTech-oplossing nog enige tijd draaien parallel aan het oude proces totdat de instelling ervan overtuigd is dat de FinTech-oplossing hetzelfde resultaat behaalt. De compliance en/of risk officer moeten worden betrokken bij de tests. Deze tests moeten aan de toezichthouder op verzoek kunnen worden overlegd.
b. De Wwft-instelling moet een schriftelijke overeenkomst aangaan met de aanbieder van de FinTech-oplossing en moet daarin afdwingen dat hij wordt geïnformeerd over alle wijzigingen met betrekking tot de oplossing en wijzigingen en ook voorafgaande goedkeuring verlangen.
c. De Wwft-instelling moet procedures hebben die voorzien in continue monitoren van de effectiviteit en werking van de FinTech-oplossing, door in ieder geval de processen te toetsen. Als er een fout wordt ontdekt, moet de Wwft-instelling: (i) alle geïnfecteerde klantrelaties beoordelen; (ii) een afweging maken of bepaalde geïnfecteerde klantrelaties of daarbij betrokken transacties moeten worden beëindigd met de kennis van nu; en (iii) een afweging maken of melding moet worden gedaan aan de Financial Intelligence Unit ('FIU') van een ongebruikelijke transactie. Het verdient aanbeveling om deze afwegingen te documenteren.
d. Wanneer een fout is ontdekt in de FinTech-oplossing, moet de Wwft-instelling – in aanvulling op de hierboven genoemde maatregelen – beoordelen of: (i) de oplossing nog wel voldoende betrouwbaar is voor de Wwft-instelling; (ii) bepaalde aanpassin-

[8] JC 2017 37, 26/06/2017. Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and firms should consider when assessing the money laundering and terrorist financing risk associated with individual business relationship and occasional transactions.

gen moeten worden gemaakt; en (iii) de oplossing kan worden voortgezet. Het verdient aanbeveling deze afwegingen te documenteren.

e. De Wwft-instelling moet maatregelen (zoals periodieke tests) treffen die waarborgen dat de instelling alle relevante informatie en documentatie ingewonnen met de FinTech-oplossing kan opslaan en bewaren. De Wwft-instelling moet op verzoek van de toezichthouders alle relevante informatie direct kunnen verstrekken.
f. De Wwft-instelling moet maatregelen treffen die datalekken voorkomen, waarbij de Wwft-instelling moet kunnen aantonen hoge standaarden te hanteren voor data en IT veiligheid.
g. De Wwft-instelling moet waarborgen dat het gebruik van de FinTech-oplossing in het klantacceptatieproces niet leidt tot strijd met privacyregelgeving, met name wanneer klantdocumentatie extern is opgeslagen. De Wwft-instelling zou dit volgens de ESA's moeten kunnen 'bevestigen' aan de toezichthouders.
h. De Wwft-instelling moet maatregelen treffen die voorkomen dat haar werknemers samenspannen met criminelen, zoals screening van nieuwe medewerkers (*pre-employment screening*). Dit is breder dan alleen ten aanzien van FinTech-oplossingen.
i. De Wwft-instelling moet waarborgen dat haar medewerkers voldoende getraind zijn om de FinTech-oplossing te kunnen gebruiken. Hiertoe moeten Wwft-instellingen periodieke training verzorgen met specifieke focus op de praktische en technische toepassing van de FinTech-oplossing en het detecteren van ongebruikelijke transacties.
j. De Wwft-instelling moet alle mogelijke compliance- en operationele risico's afwegen die zijn gerelateerd aan het gebruik van de FinTech-oplossing, zoals bijvoorbeeld een faillissement of andere opstartproblemen van nieuwe FinTech initiatieven. Dit moet in aanvulling op de algemene risicobeoordeling als bedoeld in art. 8 AMLD4.
k. Wanneer de Wwft-instelling informatie uitwisselt met de aanbieder van de FinTech-oplossing, specifiek wanneer deze gevestigd is in een derde land, moet worden vastgesteld dat dit toegestaan is op grond van wet- en regelgeving.

De ESA's vereisen van Wwft-instellingen dus nogal vergaande maatregelen alvorens een Wwft-instelling überhaupt kan overgaan tot de keuze voor een bepaalde FinTech-oplossing. Het is naar mijn mening van belang het selectieproces voor een bepaalde FinTech-oplossing zorgvuldig te documenteren, zodat dit op een later moment desgewenst kan worden overgelegd aan de toezichthouder om aan te tonen dat de instelling alle relevante factoren heeft afgewogen. Het lijkt mij ook prudent dat de Wwft-instelling een selectie maakt van verschillende aanbieders van vergelijkbare producten, om daarin een bewuste keuze te maken voor de beste FinTech-oplossing gelet op het doel dat de Wwft-instelling ermee beoogt te bereiken.

De ESA's vereisen van Wwft-instellingen dus nogal vergaande maatregelen alvorens een Wwft-instelling überhaupt kan overgaan tot de keuze voor een bepaalde FinTech-oplossing

Kwaliteit en effectieve werking van de FinTech-oplossing

Wwft-instellingen zijn op grond van AMLD4 verplicht om aan de toezichthouder te kunnen aantonen dat hun klantacceptatieprocedures evenredig zijn aan de witwasrisico's die zij lopen. Dit betekent volgens de ESA's onder meer dat een Wwft-instelling die een FinTech-oplossing wil implementeren, moet kunnen aantonen dat die oplossing voldoende betrouwbaar is en ook evenredig is met het oog op de witwasrisico's die de Wwft-instelling loopt. Volgens de ESA's moeten de toezichthouders in ieder geval de volgende factoren afwegen:

a. De Wwft-instelling moet maatregelen treffen die waarborgen dat een klantrelatie pas tot stand komt nadat het volledige klantacceptatieproces is doorlopen. De uiteindelijke keuze voor het aangaan van een klantrelatie moet bij de Wwft-instelling liggen (en dus niet bij de FinTech-oplossing), waaronder de acceptatie van hoog risicoklanten en de goedkeuring voor een klantrelatie met een PEP. Dit speelt met name wanneer het klantacceptatieproces wordt doorlopen via een FinTech-oplossing van een externe aanbieder.
b. De Wwft-instelling moet controlemechanismen hebben om de kwaliteit van het klantacceptatieproces en de gegevens en informatie die worden ingewonnen te kunnen monitoren wanneer de Wwft-instelling gebruikmaakt van een (interne of externe) FinTech-oplossing. Denk hierbij aan regelmatige tests, voortdurende compliancemonitoring, beoordelingen door de *internal audit*-functie en *on-site visits* in geval van een externe dienstverlener.
c. Wanneer de FinTech-oplossing voorziet *in* monitoring van de klantrelatie en klanttransacties, dan moet de Wwft-instelling waarborgen dat de oplossing effectief en efficiënt werkt. De oplossing moet volledig aansluiten bij de processen van de Wwft-instelling en toegang hebben tot alle informatie. De Wwft-instelling moet weten welke data en informatie wordt meegewogen door de FinTech-oplossing en moet de betrouwbaarheid van die data en informatie op waarde kunnen schatten. De FinTech-oplossing moet in staat zijn een zorgvuldige afweging te maken van ongebruikelijke transacties en moet een totaalbeeld kunnen vormen van het klantprofiel, door alle relevante informatie aan elkaar te linken.
d. De Wwft-instelling moet waarborgen dat de documentatie, de gegevens en informatie ingewon-

nen door de FinTech-oplossing in het kader van de klantacceptatie actueel blijft.

De Wwft-instelling moet dus een goed begrip hebben van het specifieke product dat hij afneemt

De Wwft-instelling moet dus een goed begrip hebben van het specifieke product dat hij afneemt. Dit betekent wat mij betreft in de praktijk dat de aanbieder van de FinTech-oplossing het product en alle kenmerken uitgebreid presenteert aan de Wwft-instelling, dat daar alle bij het klantacceptatieproces betrokken medewerkers bij betrokken zijn en dat er verschillende oefensessies gepland worden om met het product te werken.

Betrouwbaarheid van gegevens ingewonnen met de FinTech-oplossing

Wwft-instellingen moeten extra aandacht besteden aan de geldigheid en authenticiteit van de documentatie, gegevens en informatie die worden ingewonnen via video conferences, mobiele apps, of andere digitale wegen. Hierbij moeten Wwft-instellingen in ieder geval de volgende factoren afwegen:

a. De Wwft-instelling moet het risico dat het beeld van de klant op het scherm wordt gemanipuleerd zoveel mogelijk beperken. Hiertoe kan de instelling verschillende maatregelen treffen:
   - Een live chat met een medewerker die getraind is ongebruikelijk gedrag te herkennen.
   - Een ingebouwde applicatie die automatisch biometrische gezichtsherkenning toepast op basis van een digitale foto of video conference.
   - Minimale verlichting van het scherm dat wordt gebruikt voor het maken van een foto of video conference, zodat de persoon duidelijk in beeld komt.
   - Een ingebouwde applicatie die afbeeldingen kan herkennen waarin gephotoshopt is.

b. De Wwft-instelling moet voorkomen dat het getoonde identiteitsbewijs van een ander persoon is die veel lijkt op de klant. Hiervoor moeten bepaalde waarborgen zijn ingebouwd in de FinTech-oplossing die dergelijke verschillen tussen personen kunnen herkennen.

c. De Wwft-instelling moet controlemechanismen inbouwen die waarborgen dat het identiteitsbewijs niet is gewijzigd, nagemaakt of hergebruikt. Hiertoe kunnen Wwft-instellingen de volgende maatregelen treffen:
   - Ingebouwde *tools* die frauduleuze identiteitsbewijzen kunnen herkennen op basis van de (veiligheids)kenmerken van het identiteitsbewijs (watermerk, de foto, overige gegevens en de plek waar die gegevens zijn weergegeven op het document).
   - Vergelijken van de veiligheidskenmerken aan de hand van een template identiteitsbewijs.
   - Wanneer verificatie niet plaatsvindt op basis van door de overheid uitgegeven identiteitsdocumenten, een *tool* die het mogelijk maakt de van de klant verkregen informatie te controleren aan de hand van een combinatie van betrouwbare en onafhankelijke bronnen (waaronder de Kamer van Koophandel), aangevuld met analyses van *social media*, IP-adres, locatie en andere gegevens uit openbare bron.
   - Beperken van de identiteitsbewijzen die voor verificatie kunnen worden gebruikt tot bewijzen die:
     - Sterke veiligheidskenmerken hebben of biometrische gegevens zoals vingerafdrukken en een foto van het gezicht. Het lijkt mij sowieso zeer wenselijk dat het document in ieder geval een foto heeft.
     - Een gekwalificeerde elektronische handtekening gekoppeld hebben (als bedoeld in de zogenoemde eIDAS Verordening[9], waarover hierna meer). De gekwalificeerde elektronische handtekening voldoet aan bepaalde waarborgen. Er wordt een gekwalificeerd certificaat (een digitaal bestand) aan het oorspronkelijke document toegevoegd. Het certificaat is uitgegeven door een speciale instantie. Een gekwalificeerde elektronische handtekening biedt aldus extra waarborgen dat de persoon inderdaad is wie hij of zij beweert te zijn.
     - Via de FinTech-oplossing een koppeling maken met informatie uit betrouwbare en onafhankelijke bron, zoals de Kamer van Koophandel.
     - Via de FinTech-oplossing een koppeling maken met het door de overheid ingerichte stelsel voor elektronische identiteit (eID) als bedoeld in de eIDAS Verordening.

[9] Verordening (EU) Nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG. Zie voor een nadere beschouwing van de juridische implicaties van de eIDAS Verordening: J.J. Linnemann, 'Uitvoering van de verordening elektronische identificatie en vertrouwensdiensten', *IR* 2015, nr. 5/6, p. 176-181 en J.J. Linnemann, 'Uitvoering van de verordening elektronische identificatie en vertrouwensdiensten: elektronische identificatie', *IR* 2016, nr. 4, p. 134-139.

Lidstaten moeten vanaf 29 september 2018 toestaan dat Europese burgers en bedrijven zich kunnen identificeren bij organisaties in de publieke sector met behulp van een eID, uitgegeven in iedere willekeurige lidstaat van de EU

Als korte toelichting: een eID is in feite een elektronische identiteit, die de persoon in kwestie in de gelegenheid stelt zich online te identificeren. Lidstaten moeten vanaf 29 september 2018 toestaan dat Europese burgers en bedrijven zich kunnen identificeren bij organisaties in de publieke sector met behulp van een eID, uitgegeven in iedere willekeurige lidstaat van de EU. Het is dan in feite een derde (namelijk de uitgever van het eID) die garandeert jegens de organisatie waar de persoon inlogt, dat de persoon is wie hij of zij beweert te zijn. Aan de opzet van een eID zitten bepaalde waarborgen vast, zoals dat de uitgever van het eID de identiteit van de persoon heeft vastgesteld. In Nederland zijn eHerkenning[10] (voor rechtspersonen) en Idensys[11] (voor natuurlijke personen) dergelijke eID's die door de Nederlandse overheid worden ondersteund teneinde bij organisaties in de publieke sector te kunnen inloggen. Ondernemingen kunnen er tevens voor kiezen hun klanten zich te laten identificeren door deze eID's, maar dat zijn ze – anders dan de overheid – niet verplicht. Vanuit de private sector is door een gezamenlijk initiatief van banken een eID ontwikkeld onder de naam iDIN.[12] Banken zijn immers al verplicht – op grond van de Wwft – al hun klanten te identificeren.[13]

d. De Wwft-instelling moet maatregelen treffen die waarborgen dat alle ongebruikelijke transacties of patronen worden herkend. De instelling moet de output van de FinTech-oplossingen kunnen controleren op kwaliteit en vergelijken met haar eigen output tot dusver.
e. Wanneer de FinTech-oplossing wordt gebruikt voor het monitoren van de zakelijke relatie, moet de Wwft-instelling kunnen waarborgen dat alle relevante informatie en data beschikbaar is voor de FinTech-oplossing en betrouwbaar is.

Risico's vanwege het leveringskanaal (online of digitaal)

Juist in gevallen waar een onderneming een FinTech-oplossing wil integreren in het klantacceptatieproces, zal vaak geen fysiek contact plaatsvinden met de klant. Relevant in dit kader is dat AMLD4 – in tegenstelling tot de huidige Wwft en AMLD3 – niet langer voorschrijft dat in geval de cliënt niet fysiek aanwezig is voor verificatie van diens identiteit, dit per definitie kwalificeert als verhoogd risico en er altijd verscherpt cliëntonderzoek moet worden toegepast. In plaats daarvan volgt uit Annex III van AMLD4 dat het aangaan van een zakelijke relatie op afstand – zonder bepaalde waarborgen zoals een elektronische handtekening – een factor is voor een potentieel verhoogd risico. Het is dus aan de instelling zelf hier een afweging in te maken. De ESA's merken hierbij op dat Wwft-instellingen bij het onboarden van een klant via een FinTech-oplossing in ieder geval de volgende factoren moeten meenemen.

a. Bestaat er een risico dat de klant niet is wij hij of zij beweert te zijn (identiteitsfraude)? Om dit risico (dat in feite altijd aanwezig is) zoveel mogelijk te beperken, kunnen instellingen de volgende maatregelen treffen:
   - Verificatie aan de hand van een combinatie van gegevens, waaronder van het identiteitsbewijs, de informatie van de live chat en overheidsinformatie.
   - Ingebouwde *tool* aan de hand waarvan de moedertaal van een klant kan worden achterhaald op basis van schriftelijke communicatie met die klant.
   - Als voorwaarde stellen dat alle documentatie is afgegeven met een gekwalificeerde handtekening.
   - Verificatie van het adres door er een brief naartoe te sturen.
   - Verificatie van de identiteit aan de hand van een eID dat is afgegeven in overeenstemming met de eIDAS Verordening.[14]

Dit laatste lijkt mij een zeer positieve ontwikkeling. Het effect van het gebruik van een eID is dat een onderneming kan vaststellen dat een persoon is wie hij of zij beweert te zijn.[15] Wat mij betreft mag daar dus (juist) ook in het kader van de Wwft veel waarde aan toegekend worden. Die koppeling werd tot nu toe echter nog niet gemaakt, dus wat dat betreft is het naar mijn idee positief dat de ESA's die koppeling nu wel maken.[16] Het kan ook

[10] www.eherkenning.nl.
[11] www.idensys.nl.
[12] www.idin.nl.
[13] Zie voor een nadere beschouwing van de juridische implicaties van het eID het in voetnoot 10 aangehaalde artikel van Linnemann.
[14] Zie voetnoot 9.
[15] Zie ook Overweging 16 eIDAS Verordening.
[16] Overigens is de koppeling ook gemaakt in het recente FinTech Action plan van de Europese Commissie, van 8 Maart 2018 (IP/18/1403. Hierin noemt de Europese Commissie (op pagina 4): '*Additionally, the cross border recognition of electronic means of identification provided by the eIDAS Regulation will provide safeguards and mitigate risks from emerging technologies, while making it easier to meet customer due diligence anti-money laundering requirements and strong authentication of parties in a digital environment.*' En later op pagina 10: '*(...) the Commission announced its intention to facilitate the cross-border acceptance of e-identification and remote know-your-customer processes. The aim is to enable banks to identify consumers digitally in compliance with anti-money laundering and data protection*

zijn dat de ESA's hier al vooruitlopen op een voorstel van de Europese Commissie tot wijziging van AMLD4 (het 'Voorstel' en ook wel 'AMLD5' genoemd).[17] In art. 13 lid 1, onder a) van het Voorstel is expliciet aangegeven dat een Wwft-instelling de identiteit van de cliënt kan verifiëren op basis van documenten, gegevens of informatie uit betrouwbare en onafhankelijke bron, *met inbegrip van, voor zover beschikbaar, een eID zoals vastgesteld in de eIDAS Verordening*. Dat zou er dus toe moeten leiden dat indien een klant inlogt met behulp van een eID en daarmee bepaalde gegevens verstrekt aan de Wwft-instelling, daarmee ook de identiteit van de klant door de Wwft-instelling is geverifieerd. Dat neemt niet weg dat er nog additionele maatregelen getroffen moeten worden, maar het zou in potentie een lastenverlichting kunnen betekenen voor veel Wwft-instellingen (met name waar het natuurlijke personen betreft, en geen UBO of wettelijke vertegenwoordiger hoeft te worden geïdentificeerd). Het is interessant om deze ontwikkelingen nauwgezet te volgen de komende tijd.

b. Bestaat er een risico dat de klant (door een ander) onder druk is gezet gedurende het klantacceptatieproces? Dit zou natuurlijk vrij ver gaan, maar de ESA's verwachten niettemin van Wwft-instellingen dat ze controlemechanismen hebben geïmplementeerd die dwang kunnen herkennen, bijvoorbeeld door werknemers die live chats voeren te trainen op het herkennen van dwang.

Geografische risico's

Tot slot wijzen de ESA's op geografische risico's die Wwft-instellingen moeten afwegen bij digitale klantacceptatie. Wwft-instellingen moeten kunnen controleren vanuit welk land of regio de klant het klantacceptatieproces doorloopt (zoals aan de hand van GPS). Daarnaast moeten Wwft-instellingen beoordelen waarom een klant woonachtig of gevestigd in een ander land of regio juist de diensten wil gebruiken van de instelling.

Dankzij de Opinie de weg in ieder geval open ligt voor marktpartijen om FinTech-oplossingen te implementeren in hun klantacceptatieproces en transactiemonitoring

Indruk van de Opinie

In de Opinie schetsen de ESA's zeer gedetailleerde maatregelen die Wwft-instellingen moeten afwegen bij het gebruik van FinTech-oplossingen. Het voelt bijna alsof een team van knappe koppen van EBA bij elkaar is gaan zitten en alle mogelijke maatregelen heeft bedacht die men maar kan bedenken. Het positieve hieraan is dat dankzij de Opinie de weg in ieder geval open ligt voor marktpartijen om FinTech-oplossingen te implementeren in hun klantacceptatieproces en transactiemonitoring. Tot nu toe was onder omstandigheden gissen of de toezichthouders (DNB en de AFM) zich in dergelijke initiatieven konden vinden voor naleving van de Wwft. De ESA's dragen de toezichthouders nu expliciet op om deze ontwikkelen te ondersteunen, met name wanneer FinTech-oplossingen de effectiviteit en efficiëntie van naleving met de Wwft verbeteren.[18] Daarbij moeten de risico's natuurlijk ook zorgvuldig worden afgewogen. Wwft-instellingen moeten kunnen aantonen dat ze alle relevante risico's hebben geïdentificeerd, afgewogen en gemitigeerd voordat de keuze voor een FinTech-oplossing wordt gemaakt. Hier ligt dan ook een concrete uitdaging voor de Wwft-instelling. Wanneer de instelling overweegt een FinTech-oplossing te integreren in haar klantacceptatieproces, doet zij er goed aan de Opinie als checklist te hanteren, daar ook goed onderzoek naar te doen en niet blind te varen op beloftes van de makers van de FinTech-oplossing. Het proces voor de selectie van een FinTech-oplossing zou naar mijn mening goed moeten worden gedocumenteerd. Compliance officers zullen moeten waarborgen dat aan alle genoemde voorwaarden is voldaan.

Opvallend is verder dat een aantal van de door de ESA's gesuggereerde maatregelen breder toepasbaar is dan alleen maar met betrekking tot FinTech-oplossingen. Op bepaalde plekken geven de ESA's dit ook expliciet mee. Wat dat betreft biedt de Opinie dus een interessante inkijk in de maatregelen die Wwft-instellingen wat de ESA's betreft zouden moeten treffen voor naleving van de Wwft. Die gaan op het eerste gezicht nog weer verder dan de door DNB en de AFM aan de markt opgelegde maatregelen. Een voordeel is dat de ESA's vrij concrete handvatten bieden hoe marktpartijen invulling moeten geven aan hun verplichtingen op grond van AMLD4 (en daarmee de Wwft). Gelet op het risicogebaseerde karakter van de Wwft en de vele open normen, lijkt mij dat op zichzelf een positieve ontwikkeling, waarbij ik er overigens voor zou willen pleiten dat de lijst van maatregelen niet dwingend zou moeten zijn. Wwft-instellingen moeten de maatregelen treffen die zij nodig achten gelet op de specifieke risico's. Met andere woorden: als een risico zich niet of zeer beperkt voordoet, hoeft daarvoor ook geen maatregel getroffen te worden, of kan deze een lichtere invulling krijgen.

Het zou naar mijn mening ook in het belang van de markt zijn wanneer de AFM en DNB zouden uitspreken de Opinie waar relevant en waar mogelijk te volgen in hun toezicht op Wwft-instellingen. In dat

requirements, making full use of the electronic identification and authentication tools provided under eIDAS.'

[17] 2016/0208 (COD). Over het Voorstel van de Europese Commissie bereikten het Europees Parlement en de Raad een politiek akkoord over het Voorstel. Het Europees Parlement stemt 16 april 2018 over het Voorstel.

[18] Zie paragraaf 23 van de Opinie.

verband is nog relevant te noemen dat de AFM in haar agenda van 2018 heeft aangegeven te streven naar convergentie in het toezicht, om zo toezichtarbitrage te voorkomen.[19] De AFM geeft daarbij aan dat zij waar mogelijk en wenselijk zal pleiten voor meer Europese bevoegdheden voor een van de ESA's. Dit lijkt mij een zeer wenselijke ontwikkeling. Binnen deze visie past naar mijn mening zonder enige twijfel dan ook dat de AFM de Opinie van de ESA's zal volgen. Dat zou wat mij betreft ook voor DNB moeten gelden.

Slotwoord

De AFM en DNB richten zich in hun doorlopend toezicht steeds meer op naleving van integriteitswetgeving. De Wwft vraagt met haar risicogebaseerde benadering en open normen, en de steeds uitgebreidere en verdergaande uitleg daarvan door de toezichthouders (AFM, DNB en de ESA's) van Wwft-instellingen inmiddels veel meer dan alleen het opvragen van een kopie paspoort. Wwft-instellingen moeten heel zorgvuldig nadenken over hoe zij hun processen ter naleving van de Wwft inrichten. Dat blijkt eens te meer op basis van de Opinie. Niet zelden leidt dit tot hoge compliance en administratiekosten.

Er is hoop dat bepaalde FinTech-oplossingen de compliance burden wat kunnen verlichten. De Opinie doet alvast een gooi naar de mogelijkheden in dit opzicht. Dat biedt perspectief, want hierin ligt besloten dat het zeker mogelijk moet zijn om FinTech-oplossingen te implementeren voor naleving van de Wwft. Bovendien is het naar mijn mening bemoedigend dat in AMLD5 wordt voorgesteld dat de verificatie van de identiteit van de klant kan plaatsvinden aan de hand van documenten, gegevens of informatie ingewonnen door identificatie met een eID afgegeven in overeenstemming met de eIDAS Verordening. Dit past bij de huidige ontwikkelingen van meer grensoverschrijdende en digitale dienstverlening.

De ESA's leggen in de Opinie echter ook zeer nadrukkelijk de verantwoordelijkheid om naleving van de Wwft zorgvuldig te waarborgen neer bij de Wwft-instellingen, ongeacht het gebruik van een FinTech-oplossing. Instellingen mogen niet over één nacht ijs gaan bij de selectie van een FinTech-oplossing en moeten verschillende maatregelen implementeren en factoren afwegen. Dat schept dan toch weer wat onzekerheid, want *hoe* moet dat dan op een manier die de toets van de toezichthouders doorstaat? Wwft-instellingen doen er dus goed aan zorgvuldig af te wegen op welke manier zij FinTech-oplossingen kunnen implementeren in het klantacceptatieproces en de transactie monitoring en wat hun afwegingen daarbij zijn. Het is van belang het selectieproces goed te documenteren, om zo nodig later aan de toezichthouder aan te kunnen tonen waarom voor een bepaalde oplossing is gekozen. ■

[19] AFM Agenda 2018, p. 21, te raadplegen via: https://www.afm.nl/nl-nl/nieuws/2018/jan/agenda-2018.

Which digital innovations can enhance the combat of financial institutions to detect Financial Economic Crime?

S.J. van Eerten MSc EMoC & mr. K.E.J. van Heugten*

Trefwoorden: digital KYC, financial crime threat analysis, cost-efficient

Introduction

The digitalization of banking not only opens up unprecedented opportunities for individuals and organizations to conduct their business, but also for the prevention and detection of Financial Economic Crime[1] (FEC). Where Know Your Customer (KYC) traditionally is recognized as 'slack' in banking processes, digital innovations show how banks can reinvent themselves and become future-proof; both from a regulatory as well as a cost-efficiency perspective.

For years now, financial crime has become a 'stay-awake' issue for corporate directors and board members around the world. The stakes to protect corporations and society from the impact of financial crime are high. The level at which criminals are targeting financial institutions has reached an all-time high, and the likelihood of this abating any time soon is low.

The World Economic Forum Global Risk Report 2017 has placed a number of risks both directly and indirectly related to financial crime on its top 10 list of high likelihood and impact: large-scale terrorist attacks, weapons of mass destruction, massive incidents of data fraud/theft and illicit trade.[2] The report goes on to say *'slow growth, high debt and demographic change creates an environment that favours financial crises, pervasive corruption, short-termism and unequal benefits of growth'.*

Financial institutions need to look for opportunities to reduce compliance costs, enhance customer experiences and generate new business models while remaining compliant

While it's difficult to quantify the costs of financial crime for organizations, there is no doubt it has become a significant issue for financial institutions and one that is getting more challenging by the day. What is clear is that financial institutions cannot keep on top of all these dynamic threats by tackling today's incidents with yesterday's strategies. Financial institutions need to look for opportunities to reduce compliance costs, enhance customer experiences and generate new business models while remaining compliant. This article sets out how financial institutions can accomplish this with 'Digital KYC'. First the current state and trends in fighting FEC are described. Next, key elements for Digital KYC are discussed, such as Robotics, Artificial Intelligence and Smart Identity.

Financial crime threat analysis

A first step in designing an organization's approach to combat financial crime is by gaining a robust understanding of who financial criminals may be, how and where they operate, and what their motives are. This gives the organization valuable insights into which defences may be vulnerable and how they may be breached. A report[3] by the FACT Coalition says that law enforcement, policy makers and the media can get so distracted by the immediacy of criminal behaviour that it's easy to forget the goal isn't the crime itself: it's the money. The modus operandi of the financial criminal is to abuse the financial institution either to dishonestly generate wealth or to protect a benefit already obtained; and then to remain undetected and fly under the radar.

---

* Sjors van Eerten is a senior manager at Deloitte Financial Crime Advisory; Kim van Heugten is a manager at Deloitte Financial Crime Advisory. This article is written under the authors' personal titles. Views presented are personal.

1 Money Laundering, Terrorist Financing, Tax evasion and Sanction circumvention are examples of Financial Economic Crime.

2 The World Economic Forum (WEF), *Global Risk Report 2017 – 12th Edition*, Switzerland: 11 January 2017.

3 John A. Cassara, FACT Coalition, *Countering International Money Laundering – Total Failure is 'Only a Decimal Point Away'*, August 2017.

Criminals successfully abuse the financial institution when they or their wrongful activities remain undetected. Perpetuating crimes can occur in multiple ways and in recent years include the following:

- Tax evaders hid funds from tax authorities by mispresenting the identity of an account's beneficial owner and hiding a second nationality;
- Politically Exposed Persons ('PEPs') received corrupt payments by concealing their true identity by falsifying identification records;
- Financial institutions facilitated payments to sanctioned countries because they colluded with customers to manipulate SWIFT messages to obscure the true beneficiary and/or originator of the transaction;
- The (complex) transfers of crypto-currencies, which currently are not subjects of the financial supervision system; and
- Financial institutions facilitated the transportation of embargoed goods to sanctioned countries because criminals falsified records such as changing the names and flags on ships, and prevented hits on the financial institutions transaction filters.

Financial criminals are motived and persistent and identify weakness in the organization's defenses. Their methods of exploitation will adapt to the environment in which they operate, and accordingly financial institutions need to always be one step ahead

Financial criminals are motived and persistent and identify weakness in the organization's defenses. Their methods of exploitation will adapt to the environment in which they operate, and accordingly financial institutions need to always be one step ahead

Trends impacting on Financial Economic Crime

There is a strong call from customers, regulators, shareholders and society for boards of directors to proactively seek out effective strategies to protect their organizations, now and in the future. In order to improve, financial institutions need to understand a number of emerging trends in the financial services industry that have the potential to offer more opportunities for financial criminals and support for them in avoiding detection. Key external trends are:

- Heigtened customer expectations
- Increased legal and regulatory frameworks
- Maximizing profits vs. compliance costs
- Intensified competition

Heightened customer expectations

In an era of digitization, customers have continuous access to information and services. This is driven by a massive shift towards e-commerce and the rapid growth of an on-demand economy. It is this context, financial institutions nowadays are judged on their ability to deliver digital convenience and meet the customer's lifestyle. Customers desire access to waterproof mobile applications that use face and voice recognition software for identification. This is currently not widely exploited by financial institutions.

It is this context, financial institutions nowadays are judged on their ability to deliver digital convenience and meet the customer's lifestyle

It is this context, financial institutions nowadays are judged on their ability to deliver digital convenience and meet the customer's lifestyle

Although financial institutions are aware of the importance of a 'digital bank'[4], financial institutions have difficulties to successfully align their culture – system of values, beliefs, and behaviors that shapes 'how work gets done' – with the business, operations, and customer models found in digital enterprises. Key developments are:

- Variety of methods to access the financial systems, e.g. on-line banking, mobile banking.
- Innovation in products, e.g. crypto currencies.
- Speed of transaction processing, e.g. real time payments.
- Ease of access to the financial systems; opening of accounts (e.g. by shell companies).
- Increased connectivity across borders.
- Diversity of channels available in the financial system (e.g. via PSP's, e-wallets).

Financial institutions should be aware of the investments they make, or have already made, in getting customer loyalty and satisfaction by delivering the right solutions and experience. Whilst these bring about efficiencies, choices and meeting customer needs, they also bring the same advantages and opportunities to the financial criminal.

They are increasingly being held responsible for inaccurate or missing KYC information and the inability to understand internal signals that indicate deviant customer behavior

They are increasingly being held responsible for inaccurate or missing KYC information and the inability to understand internal signals that indicate deviant customer behavior

[4] In this article a digital bank refers to a bank that incorporates new and developing technologies to build deep customer relationships, enhance productivity and to provide enhanced customer services and experiences effectively and efficiently.

Increasing legal & regulatory frameworks

Over the last decade (and even more intensely the last few years) regulatory pressure has increased within the Financial Services Industry. A web of legal and regulatory frameworks has emerged globally, by country and region, which financial institutions must navigate on a daily basis – especially on topics as KYC.[5] As a consequence, financial institutions require greater granularity and accuracy in their KYC capabilities. They are increasingly being held responsible for inaccurate or missing KYC information and the inability to understand internal signals that indicate deviant customer behavior. Examples of recent KYC bottlenecks are:

- Non-adherence to KYC and AML guidelines;
- Incomplete identification and verification of source of funds;
- Failure to gain full insight in ownership structures; and
- Ineffective transaction monitoring[6].

The effect of shifted regulatory expatiations is that whilst financial institutions are forced to combat financial crime, the associated regulatory complexity becomes ever more time consuming and requires seamless adaptation into policies and procedures to avoid causing unnecessary distraction and cost to compliance staff and the business.

Maximizing profits and reducing compliance costs

Across the world, financial institutions are focusing on maximizing their profits. They are using innovation and technology in order to gain insights into their customers, people, finances and supply chains to make more effective, strategic decisions. As a part of this, financial institutions must seriously invest in their KYC activities. Not only in order to stay compliant and prevent financial crime, but also to achieve an improved, efficient and transparent control structure. The required investments result in financial challenges arising from managing KYC-related costs and, at the same time, maintaining efficiency in executing KYC controls.[7]

KYC processes and procedures lack in standardization and still include too many repetitive manual and time-consuming tasks

A substantial part of KYC costs is related to technology and data quality. Over the years, financial institutions have built up complex IT landscapes with many different systems and interfaces. For KYC this has resulted in a costly and ineffective process. KYC processes and procedures lack in standardization and still include too many repetitive manual and time-consuming tasks.

(See figure on next page)

The larger and more distributed the financial institutions become, the harder it is to access consistent, high-quality and standardized data. Poor data quality and tooling effects opportunities to understand alerts generated from internal data sets that indicate an issue, e.g. due to poor maintenance of due diligence documentation.

Intensified competition

In the Financial Service Industry technological innovation is accelerating and more and more software vendors (FinTech companies) are extending the functionalities of their solutions.[8] Although FinTechs still represent a relatively small share of the overall financial market, FinTech firms are growing rapidly. They are able to innovate in creative and fast-paced ways while established financial institutions are hampered by legacy IT-systems, processes and culture.

The companies are not well equipped to collect, share, monitor and analyze the data which provides the warning signs of malfeasance

In addition to this, the vast organizational complexity of traditional (global) financial institutions increases the threat of Financial Crime simply by virtue of their size. The real issue is not that management is hiding illicit activity, but that the companies are not well equipped to collect, share, monitor and analyze the data which provides the warning signs of malfea-

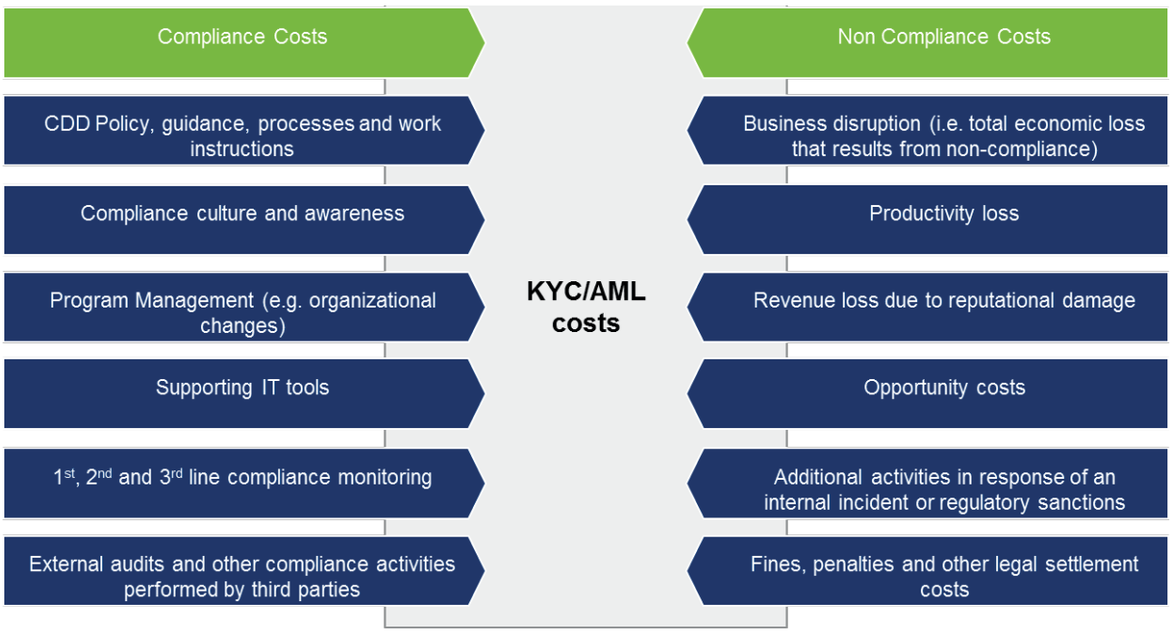
---

[5] For example, development of the 5th European AML Directive has started before the 4th AML Directive has even been implemented. Other examples are FATCA/CRS, Privacy and other regulations that are continuously changing and getting more strict and extensive.

[6] In 2017, the Dutch Central Bank published a guidance paper on the post-event transaction monitoring process at banks in which it stressed the need and desire for advanced transaction monitoring systems such as artificial intelligence. (De Nederlandsche Bank N.V. (2017), *Post-event transactiemonitoringsproces bij banken. http://www.toezicht.dnb.nl/binaries/50-236416.pdf).*

[7] KYC operations bring along significant regular compliance costs such as activities by the business, compliance and/or other supporting functions and third parties, aimed at compliance with internal and external requirements.

[8] Many FinTechs start as niche players within the Financial Services Industry and often specialize in one single product or service with which they seriously compete with established parties who are more focused on cross-selling: a total package of several interconnected products and services.



Overview of compliance and non-compliance costs

sance. Professionals share the opinion that established banks are underestimating the impact of technological innovation.[9] One of the main reasons is that the current business model of established banks has been working for over a hundred years and feels safe. This causes counteractivity of traditional trends within the bank which inhibits innovation.

It should not be overlooked that FinTechs also cause disruption to the Financial Institutions market and thereby heighten uncertainty. Financial institutions need to consider new risks associated with its interaction with FinTechs (e.g. payment service providers share less customer information in the interaction with financial institutions which limits possibilities for detecting financial crime).

Analysis of financial crime trends

This chapter showed that customers and regulators expect more commitment to addressing Financial Crime in terms of a technical response. In addition, the Financial Service Industry is currently supervised under a more stringent regulatory regime. This heavily influences the cost of complying, especially in the KYC domain. Whilst established banks have trouble to streamline and smooth their KYC processes, customers increasingly expect financial institutions to step up their game in the digital world. This is emphasized by the capabilities of FinTechs which further stress the need for digital transformation at established banks.

Digital KYC as a future proof answer

Leading up to 2025, a glimpse ahead (should) show radically transformed bank models with an emphasis on innovative technologies to facilitate banking, including:

- Inclusive banking through new types of bank models with a different, non-conventional, governance and strategy;
- Non-traditional alliances between banks and, for example, software developers or data specialists to make banking affordable; and
- FinTech capabilities to make banking more customer-centric.

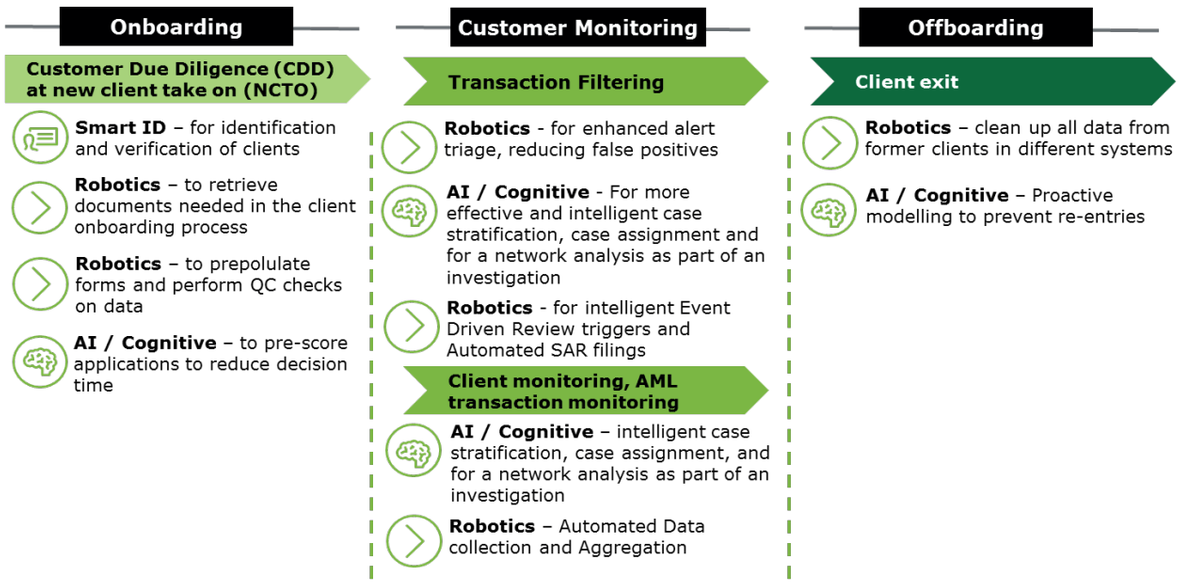
Innovation in the financial services industry is inevitable. To stay ahead banks also need to adequately meet regulatory requirements, limit compliance costs and enhance customer experiences – especially in the KYC domain

Innovation in the financial services industry is inevitable. To stay ahead banks also need to adequately meet regulatory requirements, limit compliance costs and enhance customer experiences – especially in the KYC domain.

The paragraphs below explain how the described developments can influence and change traditional banking. When discussing key digital developments, the phase of the customer life cycle within the financial institution as set out below will be taken into account.

[9] 'Banken onderschatten de impact van technologie nog altijd, zegt Cambridge-hoogleraar', *Financieel Dagblad*, 26 januari 2017.

Phases of the customer life cycle:



Overview of KYC customer life cycle with digital innovations

Robotics is best suited for processes that are repetitive and deterministic, have minimum level of ambiguity, high likelihood of human error and very few exceptions

Robotics to ease and automate processes

The spectrum of Robotics (or also called Robotic Process Automation, RPA) expands from simple rule-based automation to advanced cognitive and artificial intelligence automation. Robotics is best suited for processes that are repetitive and deterministic, have minimum level of ambiguity, high likelihood of human error and very few exceptions. Robotics should be used to mimic human interactions that are used to find and retrieve customer data based on business rules, consolidate the data and make it available in a database.
Most of robotics processes have the following characteristics:

- All processes have set defined rules with minimal or no human judgement elements;
- The manual effort in these rule-based repetitive steps is high;
- The processes are standardized from input, process steps, and output perspectives;
- Most processes have input data that is electronic (rather than paper);
- Transaction volumes of these processes are high enough to justify the automation.

From a KYC perspective, the automation of repetitive manual activities by robots is suitable for easing the following KYC activities:

- Prefill risk assessment form (including the automation of PEP and sanctions screening) based on documents delivered by the customer, and run risk indicator hits;
- Perform quality checks on data in customer administration, CRM system and customer file;
- Automate filling and updating customer administration;
- Run adverse media searches;
- Automate document upload and filing in archive;
- Highlight discrepancies in customer files;
- Automatic and intelligent event driven (and periodic) review signals;
- Delete customers from systems in case of customer exit; and
- Dashboard to visualize key findings.

Robotics can also simplify processes for off-boarding customers, such as identifying all products that a customer holds at a bank. Robots automatically search through product databases to detect related products and can automatically delete customer and related data from systems after approval has been given for off-boarding of all associated products.

The benefits of robotics in KYC include, amongst others, the following:

- Managing complex data (internal & external) gathering tasks e.g. sourcing data from multiple sources and storing it in a data warehouse to then pre-populate a KYC completion tool;
- Automatic letter generation: no need for ad hoc customer outreach which will reduce inconsistencies such as multiple outreach from different territories;

- Automatic upload of data to KYC templates rather than a manual transposition;
- Decreased cycle times and improved throughput;
- Flexibility and scalability;
- Improved accuracy and detailed data capture;
- Improved employee morale – enables them to add more value; and
- Allows time for innovation and focus on customer satisfaction.

An optimal way for financial institutions to evaluate and better grasp the potential and limitations of robotics is to implement a Proof-of-Concept or Proof-of-Value.

Human intellect is mimicked by computer systems that can recognise and understand, identify semantics, apply context and interact, reason and make decisions, learn and improve

Artificial Intelligence

Artificial Intelligence (AI) is concerned with getting computers to do tasks that would normally require human intelligence. Human intellect is mimicked by computer systems that can recognise and understand, identify semantics, apply context and interact, reason and make decisions, learn and improve. AI is a complex field of interest, with many shapes and forms. AI applications such as video suggestions, product recommendations, spam filters and navigation systems have already become part of our day-to-day lives. From a KYC perspective, it could mainly be used to detect deviant behaviour in customer monitoring processes. Financial Crime detection can hugely benefit from advancement in AI to make it more flexible and scalable. Further, using location intelligence to augment AI can identify transaction anomalies, verify customer place of business and flag sensitive cross-border conditions and proximity risk.

Our increasingly sophisticated understanding of how the human brain works and our ability to embed brain-like elements into computers have engendered several capabilities that give rise to significant opportunities for easing KYC processes and improving customer satisfaction. Below are some examples of the application of AI in KYC processes are discussed.

1. Facial recognition
   A new payment technology application uses biometrics like fingerprints or facial recognition to verify a customer's identity. This technology eliminates the need for customers to recall passwords - dramatically speeding up the digital checkout experience while also improving security. Instead, the customer can verify their identity using the fingerprint scanner on their smartphone or via facial recognition technology by taking a 'selfie' photo.
2. Voice recognition
   A mobile banking app allows voice activated payments (voice controlled banking). Customers will be able to see their recent transactions and report a lost bank card, just by talking to their phone. They can also instruct the bank to pay someone – only people on their existing payee list. Transactions appear in real time once payments are made, as if they were being done manually.
3. Network analysis & pattern recognition
   For years, financial institutions have operated sophisticated systems for monitoring, investigating and reporting suspicious money laundering (AML) transactions. These systems sift through significant amounts of data and flag many transactions that require investigation as potentially suspicious activity. Financial institutions should use financial crime analytics to improve these systems, which can result in more efficient, effective, and insightful operations. Governmental regulators also exert pressure on institutions to improve monitoring and more effectively filter suspicious activities. A low cost opportunity that is often overlooked by financial institutions is to better leverage existing information generated by transaction monitoring systems and suspicious activity reporting processes. With help of AI this existing information can be analyzed to find opportunities for fine-tuning those systems to more effectively identify potentially suspicious customer behavior.

By restructuring that existing information and using network analytics to investigate it, new ways of improving the automated compliance systems may be uncovered

By restructuring that existing information and using network analytics to investigate it, new ways of improving the automated compliance systems may be uncovered. The process of Financial Crime Analytics is a mix of automated and manual activities that enhance improvements in quality and efficiency. In the process of Financial Crime Analytics several methods to detect deviant activities are applied:

- Explorative network analysis (amongst others: methods of ranking, outlier detection, cluster analysis);
- Risk ruling (so-called 'knock-out' criteria, scoring modelling, etc.);
- Predictive modelling (machine learning based on designated risk indicators, historic data and continuous adaption).

This process consists of 3 main phases:

1. Structuring and cleansing existing data and relevant databases: in phase 1 an inventory of alerts and reports of suspicious transactions, including their unique identifiers, is created.
2. Detection scenario analysis: in Phase 2, the now-structured, historical suspicious transaction information is analyzed. Objectives are to:
   a. Evaluate effectiveness of detection scenarios;
   b. Mine for undetected patterns;
   c. Tune detection scenario thresholds; and
   d. Focal entity vs. counterparty alert analysis.
3. Application of threshold refinement and system improvements: in Phase 3 the insights gleaned from Phase 2 analyses can be applied to threshold refinements and system improvements.

Financial institutions can potentially benefit from applying network analytics and data-mining tools using the methods mentioned above. AI can allow institutions to judge the overall effectiveness of their monitoring system and processes. Analytics also gives institutions opportunities to leverage investments they may have made by deriving new insights from their data.

Smart Identity

Traditional customer onboarding procedures may mean walking into a bank and going through an interview process just to open a new bank account. The costs related to these onboarding processes are relatively high. Further, in financial institutions onboarding activities are often duplicated and repeated across the organization. From a customer perspective, a customer has to provide the same identity documentations to multiple organizations. Yet customers expect quick and seamless service through multiple channels.

Identifying who is who online has become the basis for digital business. Due to place-independent commerce it has become a necessity to identify customers online. Inherently there is always a risk that online merchants lose part of their business due to identity fraud. Smart identity management could be a solution in this.

A Smart ID is a digital identity record supporting secure storage, maintenance and verification of any digital identity data. This is composed by a number of discrete service modules that can act independently, facilitating reuse across business functions helping to eliminate redundancies and thereby lowering costs

Smart Identity is a distributed identity platform within which individuals, organizations and even Internet of Things devices can create, manage, share and verify identity credentials within a secure and widely accessible environment. Smart Identity functions as a digital account containing the information and credentials needed for trusted digital interaction. A Smart ID is a digital identity record supporting secure storage, maintenance and verification of any digital identity data. This is composed by a number of discrete service modules that can act independently, facilitating reuse across business functions helping to eliminate redundancies and thereby lowering costs.

For customers the main benefit is their information is verified once. Either by the originating party or by a certified third party agency (the custodian). A blockchain solution ensures integrity and security, with access granted on an attribute and/or consumer level. It enables storing personal consumer events in a secure environment available to all connected parties in a blockchain network so that information (e.g. personal info, salary, assets) could be verified by respective institutions.

For financial institutions Smart Identity generally leads to more efficient onboarding and ongoing due diligence processes. A number of business areas that could get a much-needed boost from these Digital Identity networks are:

- Operations: digital attribute transfer and handling let financial institutions streamline and automate many processes, eliminating human error.
- Security: the secure, digital storage of user information reduces fraud resulting from stolen information or compromised authentication.
- Compliance: thanks to digital attribute handling and greater access to user identity, compliance becomes easier and more accurate.

To build a resilient Digital KYC organization, boards and senior management need to adopt a different, flexible operating model that stresses constant evolution and adaptability for a fluid and ever-evolving set of financial crime challenges

Building a resilient Digital KYC organization

While financial institutions, on the one hand, are struggling with regulatory pressure and limiting compliance costs, on the other hand this also limits a financial institution's ability to serve its customers to their full satisfaction and to focus on the customer experience.

To build a resilient Digital KYC organization, boards and senior management need to adopt a different, flexible operating model that stresses constant evolution and adaptability for a fluid and ever-evolving set of financial crime challenges. A number of things are of importance here:

- The organization requires an appropriate tone at the top and to have it articulated through the chain of command.
- The financial crime component should be built into the company strategy that stresses reputation management and a rapid response protocol to help executives make informed decisions about financial crime. Business strategy and targets should be aligned with the compliance strategy, i.e. sales targets are realistic within the compliant landscape.
- Often responsibilities for different types of financial crime sit in different parts of the organization, with little coordination or cooperation. This makes responses incomplete and can leave one part of the organization exposed to additional risk even if the immediate problem has been handled. Breaking down of silos and taking a cross-organization view of customers and transactions also makes it harder for criminals to exploit gaps between the business systems, databases and countries. A holistic approach with centralized efforts for preventing, investigating and remediating financial crime increases the effectiveness of different initiatives.
- Improve the agility and skills of the compliance organization, and create an environment that can respond to risks of today and the future rather than the past. Perform an assessment of its current operation state and set a vision for the future state. Develop a roadmap for the transformation in order to achieve the vision, and outline a target operating model. Particularly, focus on:
  - Governance: clear roles and responsibilities, and independent governance.
  - Policies: timely updates to emerging regulations.
  - Processes: consistent manner in which risk is measured / managed.
  - People: refresh of key roles, away from legal/ex law enforcement, to talent that is capable of completing more analytical and critical assessments and linking threats across the organization. Seek those that embrace complexity.
  - Technology: invest in technology that will improve and standardise data to increase capacity to perform centralised analysis. Use the latest analytics techniques which make it possible to derive insights from structured and unstructured information sources or data from disparate systems across the enterprise. The disparate systems need not only help predict problems - they can also learn as they go. Allow time for proof of concepts, testing and customisation, rather than only using 'plug and play' technologies.
  - Culture and ethics: foster an open, trusting and honest environment where staff are happy to raise and report concerns. Organizations should create a learning culture, where training is relevant and timely, and mindfulness and curiosity are encouraged and rewarded.

Where KYC traditionally is recognized as 'slack' in banking processes, new digital innovations show how banks can reinvent themselves and become future-proof, both from a regulatory as a cost-efficiency point of view

Leveraging lessons learned

The stakes to protect corporations and society from the impact of financial crime are high. Where KYC traditionally is recognized as 'slack' in banking processes, new digital innovations show how banks can reinvent themselves and become future-proof, both from a regulatory as a cost-efficiency point of view.

Financial institutions should include dedicated financial crime resources and technology competencies in the organization to be resilient for financial crime. Digital KYC solutions as Robotics, Artificial Intelligence and Smart Identity will help to digitize the KYC value chain and thus reduce compliance costs and enhance customer experience.

Our insights as described above can provide financial institutions with the opportunity to leverage the information that they already have in order to meet an unrelenting imperative they face every day: fulfilling their regulatory duty by running high quality, dynamic, and effective compliance programs – and keep this cost efficient.

However, it should be noted that the digital transformation should be executed with care - technology advancements create business opportunities, including financial crime compliance efficiencies, but they are also fueling financial crime threats. The threat and impact of financial crime will only accelerate, making resiliency in the face of financial crime a critical imperative for the long term success of any organization. ■

Kritisch over ... een proefschrift over de consumentenkredietovereenkomst

J.J.A. Braspenning, *Een gedragswetenschappelijk perspectief op de consumentenkredietovereenkomst*, Zutphen: Uitgeverij Paris 2017 (375 bladzijden, incl. onder meer een *Summary* en literatuurlijst, ISBN 978-94-6251-151-4)

prof em. mr. Antoni Brack*

Dit is de handelseditie van het proefschrift waarop Jurgen Braspenning op 24 november 2017 te Tilburg promoveerde tot doctor.
En om maar meteen met de deur in huis te vallen, het is een heel goed proefschrift met een misleidende titel. Want het boek bevat niet 'alleen maar' een gedragswetenschappelijk, maar ook een breed geschetst juridisch perspectief op de overeenkomst van consumentenkrediet. Dus wie vooralsnog alleen belangstelling zou hebben voor een analyse van de regelgeving voor consumentenkrediet laat, uitsluitend afgaand op de titel, het boek ten onrechte onaangeroerd.

Juridisch kader

Hoofdstuk 2 beschrijft het juridische kader waarin informatieplichten, waarschuwingsplichten en de kredietwaardigheidstoets belangrijke onderdelen zijn. Het is een uitgebreide verhandeling en de schrijver heeft geprobeerd de lezer te loodsen door dit doolhof van publiekrecht, privaatrecht en zelfregulering door regelmatig tussenconclusies te formuleren. Zodat we af en toe even op adem kunnen komen. Hij heeft echter ook gemeend dit overzicht aantrekkelijk te maken door zo nu en dan een 'Intermezzo' in te lassen; een uitstapje naar een belendend perceel waardoor de lezer weer van de hoofdroute wordt afgeleid. Het is ook nooit goed.
Afgezien van de vraag of het terecht is of niet, valt mij als betrekkelijke buitenstaander van tijd tot tijd weer eens op hoe alomvattend, ja bijna wurgend en ingrijpend het financiële regelkader is. Een goed voorbeeld is het toezicht op de zo geheten productontwikkeling. Voor de vraag of er wel goede financiële diensten worden ontwikkeld en aangeboden heeft de AFM zogenoemde KNVB-criteria opgesteld. Is het product, wat natuurlijk eigenlijk een dienst is, Kostenefficiënt (waarmee iets anders bedoeld wordt, namelijk of je als klant waar voor je geld krijgt), heeft het Nut (is er behoefte aan, lost het een probleem op?), is het Veilig (gaat de consument er misschien aan failliet?) en is het Begrijpelijk (snapt de klant het ook?).

Klopt het allemaal wel?

Hoofdstuk 3 is getiteld 'De beperkingen van het bestaande informatieparadigma'. Een paradigma is een *mindset*[1], de kernopvatting is dat als je er voor zorgt dat consumenten voldoende informatie krijgen, dat ze dan in staat zijn de goede beslissingen te nemen. Schrijver twijfelt hieraan onder verwijzing naar 'de schuldenproblematiek onder Nederlandse huishoudens' (p. 115), die deze twijfel zou bevestigen. Ik moet de neiging bedwingen om de relevantie van deze vergelijking van

* Antoni Brack is emeritus hoogleraar Bedrijfsrecht, Universiteit Twente en consultant Juridische bedrijfsvoering (ABC Antoni Brack Consulting). Schrijver dezes bedankt Wim Lieve (LieveComplianceConsulting) voor het kritisch lezen van de concepttekst voor dit stuk en voor suggesties tot verbetering.

[1] Vrij naar www.woorden.org.

[2] De informatieplichten van de kredietverstrekker zouden er best eens op gericht kunnen zijn om de consument het voor hem meest geschikte kredietproduct te laten

kanttekeningen[2] te voorzien, want dat zou de aandacht ervan afleiden dat dit onderwerp de echte meerwaarde van dit boek belooft te zijn, hoe dan ook.
Sluiten de juridisch afgedwongen en afdwingbare informatieplichten eigenlijk wel aan op gedragswetenschappelijke inzichten over consumentengedrag inzake krediet? De discutabele dominante opvatting is dat hoe meer informatie de consument heeft, des te beter zal de beslissing zijn. Daaraan ligt de veronderstelling ten grondslag dat hij de gestandaardiseerde informatie over de financiële dienst begrijpt en in staat is die te gebruiken voor een verantwoorde beslissing. De volledig rationeel handelende consument dus, althans volgens het geloof van veel economen, klassiek of neoklassiek. Economie lijkt veel op religie. Een zodanige consument bestaat natuurlijk helemaal niet en daar hebben andere economen iets op gevonden: de gedragseconomie. Niet omdat de (neo)klassieke economie koos voor verkeerde uitgangspunten, maar omdat beleidmakers en regelmakers ten onrechte van de rationele mens zijn uitgegaan. Begrijpt u wel?
Het is grappig om vast te stellen dat sommige door schrijver aangehaalde auteurs van de weeromstuit dan weer de neiging hebben naar de andere kant door te slaan. Ze beweren bijvoorbeeld dat mensen geneigd zijn om niets te doen en uitstelgedrag gaan vertonen (p. 127). Het paradigma van de luie consument, zeg maar.

To the point

De auteur besluit tijdig om de algemene veronderstellingen over economisch consumentengedrag maar te verlaten en een specifieke toepassing te maken voor consumentenkrediet onder de mooie subtitel 'De levensloop van een informatieplicht' (p. 129 e.v.).
Er zijn stadia te onderscheiden van informatie zenden en ontvangen. Ontvangers moeten kunnen lezen om informatie tot zich te nemen. Dat is geen open deur, want ons land telt ongeveer 250.000 analfabeten (p. 135). En mensen die kunnen lezen doen dat heel vaak niet; de aangeboden informatie wordt genegeerd. Een voor de hand liggende verklaring hiervoor is dat mensen in algemene zin veel meer informatie aangeboden krijgen dan ze in een redelijke hoeveelheid tijd kunnen verwerken. Het is bovendien goed dat we ons realiseren dat verwerken in de zojuist bedoelde zin een optelsom is van lezen en begrijpen. Schrijver vermeldt daarom ook aantallen laaggeletterden en zogenoemde laaggecijferden (p. 142). Specifiek ten aanzien van kredietinformatie komt daar nog eens financiële ongeletterdheid bij: een gebrek aan financiële kennis en vaardigheden. Deze mensen betalen bijvoorbeeld te veel voor een creditcard.[3] Mensen die qua kennis en vaardigheden wel voldoende in huis hebben hanteren gereedschappen in een poging de hoeveelheid informatie hanteerbaar te houden, zoals vuistregels en vooroordelen.[4] Hiermee kunnen keuzes sneller gemaakt worden, maar de kans dat die suboptimaal zullen zijn neemt toe. Schrijver bespreekt een aantal van wat ik hier gereedschappen heb genoemd en schetst het verloop van empirisch onderzoek hierover.

Alternatieve benaderingen

Het laatste paragraafje van het derde hoofdstuk is cruciaal voor het verdere verloop van dit promotieonderzoek en proefschrift. Ik denk dat schrijver zich hier van een vuistregel op het vlak van de waarschijnlijkheid bedient: als je radicale hervormingen voorstelt, is de kans groot dat ze niet zullen worden doorgevoerd. Hoewel de studie tot nu toe sterke aanwijzingen oplevert voor de onjuistheid van het informatieparadigma als uitgangspunt of leidend principe, stelt schrijver niettemin 'dat er nog voldoende innovatie kan plaatsvinden binnen het informatieparadigma' (p. 162). Zijn argumentatie hier is mager en zo lijkt het in hoge mate gebaseerd op pragmatische veronderstellingen. Als je dat paradigma zou loslaten dan zou dat leiden tot hoge compliancekosten voor ondernemingen. Kredietaanbieders neem ik aan. Maar als ik zo vrij mag zijn mijnerzijds een tussenconclusie te formuleren: wat denk je van de kosten van het vasthouden aan informatieplichten, die in onvoldoende mate een gewenst effect hebben?
Uitgangspunt van het vierde hoofdstuk is, hoe dan ook, dat marginale veranderingen gewenster zijn dan radicale.

Valkuilen

De alternatieve benaderingen die in dit vierde hoofdstuk de revue passeren, moeten vangnetten zijn om te voorkomen dat consumenten in een van

kiezen, terwijl geen rem wordt gezet op de aangeschafte hoeveelheid van die kredietproducten.

[3] Naar verluidt is uit onderzoek gebleken dat veel mensen meer tijd besteden aan het vinden van een *smartphone* of *laptop* dan aan het vinden van een hypotheek.

[4] In het wetenschappelijke onderzoekjargon: *heuristics* en *biases*.

de drie valkuilen terecht komen: informatie niet lezen, niet begrijpen of onbewust een verkeerde beslissing nemen.[5]
Een van de opmerkelijkste remedies die wordt besproken is het aanbieden van financiële scholing aan consumenten, niet door kredietverschaffers maar door onderwijsinstellingen. Schrijver vermeldt onder meer een groot Braziliaans onderzoek en een kleiner Duits onderzoek over het aanbieden van financiële scholing aan scholieren. Ook komt scholing van Mexicaanse en Amerikaanse consumenten aan de orde. In sommige gevallen werden de scholingskosten, opmerkelijk genoeg, doorberekend aan de kredietverstrekker!

Een andere remedie die in dit hoofdstuk wordt besproken is de waarschuwingsplicht. Daar hebben wij er in ons land eigenlijk maar een van: 'geld lenen kost geld'. De effectiviteit van deze als mededeling vermomde waarschuwing is in opdracht van de AFM onderzocht. Even kort door de bocht: er is geen effectiviteit, de waarschuwing heeft geen effect. Ik vind zo'n buitengewoon belangrijke conclusie nogal schokkend. We leggen kredietverstrekkers een wettelijke waarschuwingsplicht op, ooit bedacht door iemand in de politiek of de ambtelijke bureaucratie die een ideetje voelde opkomen en jaren later stellen we vast dat het nauwelijks of geen effect heeft. Moeten we niet eens de omgekeerde volgorde aanhouden? Eerst eens onderzoeken wat waarschijnlijk het gewenste effect heeft en dat dan daarna pas invoeren? Gelukkig hebben we dit proefschrift nog! Ik heb vertrouwen in de aanpak van de auteur als ik het volgende lees. 'Dat het lenen van geld niet gratis is lijkt mij niet het grootste risico van kredietproducten. Overkreditering is daarentegen wel een serieus risico bij het lenen van geld.' (p. 219). Hij verwijst al vast naar zijn vijfde hoofdstuk voor het vervolg. Ik kan niet wachten.
Maar eerst moeten we het nog over *nudging* hebben want dat hoort er tegenwoordig bij; het is trendy als je gedrag wilt beïnvloeden en als je het er niet over hebt, loop je het risico niet serieus genomen te worden. OK, even dan. Wat is het? Het is een steuntje in de rug, een duwtje in de goede richting. Zoals je bij kleuters doet, maar dan voor volwassenen.
Een veel voorkomende toepassing in ons digitale tijdperk is de *default*, de voorkeursinstelling: er staat al aangevinkt wat je zou willen. Een mooi inzicht is dat je al het privaatrecht dat aanvullend[6] is, als een *default* kunt zien: het zijn regels die gelden als partijen geen eigen afspraken hebben gemaakt (p. 227).

Eigen empirisch onderzoek

In het vijfde hoofdstuk wordt op begrijpelijke wijze het eigen onderzoek van schrijver stap voor stap uiteengezet en toegelicht. Bij het presenteren van de resultaten wordt het hier en daar wel wat te (onderzoek)technisch, maar de gerapporteerde resultaten zijn goed te volgen en ook wel bijzonder in de zin van verrassend. Maar om de lezer te stimuleren zelf het boek ter hand te nemen – *nudge, nudge* –, ga ik niet alles verklappen.
In het zesde en voorlaatste hoofdstuk probeert schrijver een brug te slaan tussen zijn onderzoeksresultaat en de bestaande wetgeving. Hij laat mogelijkheden tot aanpassing zien, maar doet jammer genoeg geen voorstellen. Dat laat hij liever over aan beleidmakers. 'Het is aan hen om knopen door te hakken over de invoering van een eventuele nieuwe informatieplicht.' (p. 326).
Het laatste, zevende hoofdstuk is getiteld Conclusie en is eigenlijk een samenvatting. Hieruit komt de eerder al gesignaleerde tegenstrijdigheid nog eens pregnant naar voren: hoewel veel consumenten aangeboden informatie niet lezen, bepleit schrijver toch het beschikbaar stellen van alternatieve kredietinformatie. Tegen beter weten in of toch in de hoop dat alternatieve informatie wel gelezen zal worden? 'Mijn aanbevelingen komen er samengevat op neer dat er binnen het informatieparadigma ruimte voor verbetering is.' (p. 343).

Afronding

Het doen van promotieonderzoek en het schrijven en verdedigen van een proefschrift heeft tot doel te laten zien dat iemand in staat is tot zelfstandige wetenschapsbeoefening; de doctorandus is doctor geworden. Jurgen Braspenning heeft laten zien dat hij in wetenschappelijk opzicht tot veel in staat is: zijn dissertatie is breed en diep. Heel waardevol zijn het tweede hoofdstuk over het juridische kader van de kredietovereenkomst met consumenten en het derde en het vierde hoofdstuk over de gedragswetenschappelijke aspecten. Dit zijn specialis-

[5] Deze derde categorie vind ik lastig. Mensen besteden ook bewust te weinig tijd aan het tot zich nemen en verwerken van informatie en nemen dan een verkeerde beslissing.
[6] Dit deel van het privaatrecht wordt ook wel regelend recht genoemd, een term die beter vermeden wordt omdat het een pleonasme is: alle recht is immers regelend.

tische overzichten die een zeer volledige indruk maken. Eigenlijk moet iedereen dit lezen die beroepsmatig of anderszins de indruk wil wekken te weten waar hij of zij het inzake consumentenkrediet over heeft. Dat onze jonge doctor binnen zijn specialisme ook generalist is, blijkt uit zijn bewonderenswaardig brede aanpak. Juridische, gedragseconomische en psychologische inzichten worden met elkaar in verband gebracht. En dan ook nog een eigen bijdrage toevoegen aan het empirische onderzoek op dit gebied!

Een voorbestemd breed talent, zo lijkt het wel. Want in het woord vooraf sluit hij als volgt een periode af. 'Een periode die, strikt genomen, begon toen ik mij in september 2005 aanmeldde als student aan de economische faculteit. Ik had net mijn vwo-diploma behaald en was voornemens om bankier te worden. Twaalf jaar later verlaat ik deze instelling als gepromoveerd jurist en ga ik aan de slag als advocaat. Het kan verkeren.' Dat kun je wel zeggen! Je wilt bankier worden en je promoveert op allerlei aspecten van consumentenkrediet. Zijn brede talent kwam onlangs ook tot uiting als scheidend redactiesecretaris van het Tijdschrift voor Consumentenrecht & handelspraktijken. In die hoedanigheid was hij mede verantwoordelijk voor de publicatie van een speciaal nummer (2017-6) van dit tijdschrift dat gewijd is aan consumentenrecht en de invloed van gedragswetenschappen.

Er is misschien nog in ander opzicht sprake van predestinatie. Je mag eigenlijk geen grappen maken over familienamen, maar soms is de verleiding te groot. Dat iemand die Braspenning heet op zeker moment bankier wil worden, is natuurlijk niet zo raar. In de zestiende eeuw is er een zilveren munt ter waarde van tien duiten die braspenning heet. Als dat je achternaam is dan heb je wat met geld. *Nomen sit omen*, de naam is een teken. Die munt vertegenwoordigde bovendien de waarde van de belasting op bier.[7] Bij kwesties van consumentengedrag gaat het vaak over een stortvloed van productinformatie en een overweldigend aanbod. Die ervaring had de jonge doctor zelf ook. Want ik lees (op p. 141): 'Zo bezoek ik zelf af en toe een winkel in speciale biersoorten en de bijna oneindige keuze daar doet mij iedere keer weer duizelen.' Dat kan toch geen toeval zijn? ■

[7] Bron: http://etymologiebank.nl.

Uit de boekenkast van de bedrijfsethiek (68)

dr. E.D. Karssing*

Trefwoorden: kunstmatige intelligentie, moreel kompas, ethical impact assessment

In de bedrijfsethiek is een groot aantal boeken en artikelen verschenen waarin op praktische wijze integriteitsvraagstukken worden behandeld en concrete aanbevelingen worden gedaan voor het bevorderen van de ethiek en integriteit van organisaties en hun medewerkers. Niet iedereen weet deze publicaties te vinden of heeft tijd ze te lezen. Daarom kijkt Edgar Karssing geregeld voor het *Tijdschrift voor Compliance* in de boekenkast van de bedrijfsethiek en bespreekt hij een artikel of boek. Deze bijdragen zijn geen recensies, maar een samenvatting van de belangrijkste conclusies en aanbevelingen van de auteur(s), die hij zal confronteren met zijn eigen observaties als onderzoeker, trainer en adviseur op het gebied van ethiek en integriteit.

In dit nummer wordt de ethiek van kunstmatige intelligentie besproken. Leidend hierbij zijn de boeken *Het tweede machinetijdperk. Hoe de digitale revolutie ons leven zal veranderen* van Erik Brynjolfsson en Andre McAfee, *Humans need not apply. A guide to wealth & work in the age of artificial intelligence* van Jerry Kaplan, *Life 3.0 Mens zijn in het tijdperk van kunstmatige intelligentie* van Max Tegmark, het rapport *Opwaarderen. Borgen van publieke waarden in de digitale samenleving van* het Rathenau Instituut en het artikel *A framework for the ethical impact assessment of information technology* van David Wright.

1. Inleiding

'De digitalisering van de samenleving verlegt de grenzen van ons kunnen en biedt allerlei mogelijkheden, maar daagt ook onze morele grenzen uit'.[1]

... Er komt heel wat op ons af.
... Oh? Wat bedoel je? Wat, waarmee?
... Met de digitale samenleving.
... Ah, je bedoelt de AVG, die nieuwe privacywetgeving. Ja, dat is een hoop gedoe. En veiligheid, cyber security. Dat kost ons ook nog heel wat hoofdbrekens.
... Dat is nog maar het begin. Dat is vooral gericht op dataverzameling en opslag. Belangrijker is dat we aan de vooravond van het tweede machinetijdperk staan.
... Het tweede machinetijdperk?
... Ja, het eerste tijdperk begon met de industriële revolutie. Dankzij machines waren we vanaf toen niet meer afhankelijk van de spierkracht van mens en dier. In het tweede machinetijdperk doen computers en andere digitale ontwikkelingen 'voor onze geest (het vermogen onze hersens te gebruiken om onze omgeving te begrijpen en te vormen) wat de stoommachines en de daaropvolgende apparaten voor onze spieren hebben gedaan'.[2]
... Ja geweldig, we leven in mooie tijden. Bedenk eens wat een mogelijkheden dat allemaal biedt voor het vinden van de juiste klanten, voor het verbeteren van de dienstverlening aan klanten, voor *customer loyalty management*, voor het bepalen van de prijs, voor robo-advies, voor preventie, voor het bestrijden van fraude, voor AML/klantidentificatie, voor het optimaliseren van operationele processen, voor het verminderen van risico's en het creëren van commerciële kansen. Meer omzet, meer tevreden klanten![3]

Wie doet straks het werk nog als de techniek zowel spierkracht als denkkracht overneemt?

... Dat is één kant van het verhaal. Maar wie doet straks het werk nog als de techniek zowel spierkracht als denkkracht overneemt? Kaplan maakt een sinister grapje: 'Will the last human dismissed please turn off the lights? Actually, no need – they can turn themselves off'.[4]

* Edgar Karssing is als universitair hoofddocent beroepsethiek en integriteitsmanagement verbonden aan Nyenrode Business Universiteit. De auteur dankt Olga Crapels, Wim Lieve, Sacha Spoor, Raoul Wirtz, Marc de Droog, Jos Schaffers, Lucianne Verweij, Ronald Heijn en Ronald Jeurissen voor hun commentaar op het concept van deze bijdrage. Voor reacties en suggesties: e.karssing@nyenrode.nl.

1 L. Kool, J. Timmer, L. Royakkers en R. van Est, *Opwaarderen. Borgen van publieke waarden in de digitale samenleving*, Rathenau Instituut 2017: 46.

2 E. Brynjolfsson en A. McAfee, *Het tweede machinetijdperk. Hoe de digitale revolutie ons leven zal veranderen*, Lannoo 2014: 16.

3 Zie bijv. J. van Schoonhoven, 'Big Financials, Big Data? Over wetstoepassing en morele oordeelsvorming', *Tijdschrift voor Compliance* 2014, nr.5, p. 285-291; F. Segers, 'De compliance officer en innovatie; technologie, risico's en kansen', *Tijdschrift voor Compliance* 2017, nr. 2, p. 76-83; L. de Boer (2016), *'Big Data vraagt om big ethics'*, rede uitgesproken op 21 september op Big Data Expo 2016.

4 J. Kaplan, *Humans need not apply. A guide to wealth & work in the age of artificial intelligence*, Yale University Press 2015: 11.

... Heerlijk, dan bereiken we eindelijk de heilstaat van Karl Marx: in de ochtend jagen, in de middag vissen en in de avond filosoferen. Het paradijs zoals John Maynard Keynes dat bijna 100 jaar geleden heeft voorspeld in zijn prikkelende essay *Economic Possibilities for our Grandchildren:* de 15-urige werkweek. En verder heel veel tijd voor onze hobby's.
... Doe er maar luchtig over. Wie zegt dat jij straks bij de winnaars hoort? De tweedeling neemt nu al toe. Straks hebben we een paar heel rijke mensen en verder alleen nog maar paupers. De 99 procent.
... Joh, wat maak jij je druk. Alsof wij enig invloed hebben op de toekomst. De technologie gaat toch zijn eigen gang. Tot nu toe wordt het vooral leuker. En ach, de transformatie van een boerensamenleving naar de huidige samenleving ging toch ook vrij probleemloos?[5] Eerst was ruim de helft van de bevolking werkzaam in het boerenbedrijf, nu minder dan 2 procent. Heb jij grote volksopstanden gezien, een werkloosheid van bijna 50 procent? De economie lost dat wel op.
... Nou, over die transformatie hebben we 200 jaar kunnen doen. Dat is niet vergelijkbaar met de huidige techno-revolutie. Die tijd is ons echt niet gegund. En er staat nog veel meer op het spel. Wat gaat dit allemaal betekenen voor de kwaliteit van ons leven, voor de kwaliteit van onze samenleving? Voor de menselijke waardigheid, voor onze vrijheid, voor solidariteit, voor rechtvaardigheid?
... Poeh, wat een grote woorden allemaal. Vast heel belangrijk. Maar waarom zou een compliance officer zich daar druk over maken? Een financiële instelling? Daar hebben we toch de overheid voor, laat die maar eens wat nuttigs doen met mijn belastingcenten en ervoor zorgen dat het een beetje leuk blijft voor ons allemaal.
... Het raakt ons allemaal. Als instelling, als mens, maar zeker ook als compliance officer.
... Leg eens uit.
... Volgens steeds meer mensen is de financiële instelling van de toekomst – een bank, een verzekeraar, een pensioenfonds, een trustkantoor – een ICT bedrijf. FinTech zal de manier waarop we met geld omgaan vereenvoudigen en versnellen.[6] De techniek die hier achter zit roept allemaal nieuwe ethische vragen op waar we nog nauwelijks een antwoord op hebben. Hoe ziet ons morele kompas eruit? Tot hoever strekt onze verantwoordelijkheid? Zonder antwoorden op die vragen zal het noodzakelijke vertrouwen van het grote publiek met een paar incidenten als sneeuw voor de zon verdwijnen.
... Ok. En verder?

Heeft het nog zin om parkeergarages te financieren als met zelfrijdende auto's straks niemand meer een eigen auto heeft?

... Ons morele kompas speelt ook een rol bij klantacceptatie. We willen immers niet iedereen als klant. Hiervoor kijken we ook naar de moraliteit van de producten en diensten die onze klanten aanbieden. De tabaksindustrie, prostitutie, wapenhandel. Daar hebben we een beeld bij. Maar hoe beoordelen we heel nieuwe producten en diensten die gebruik maken van blockchain, kunstmatige intelligentie en robots, als we niet eerst ons eigen standpunt hieromtrent bepalen? En heeft het nog zin om parkeergarages te financieren als met zelfrijdende auto's straks niemand meer een eigen auto heeft en deze dus ook niet meer hoeft te parkeren?
... Dan kunnen al die zelfrijdende auto's daar toch parkeren?
... Ik zou het maar serieus nemen. En hoe zit het met de 'compliance officer 3.0' die 'met behulp van *big data* en IT de toegenomen diversiteit van werkzaamheden beheersbaar en uitvoerbaar houdt'?[7]
... Zeg je nu dat ook de compliance officer zijn baan kwijt kan raken?
... Nee, ik zeg dat ook de compliance officer steeds meer gebruik zal maken van nieuwe technieken. En dan is het wel zo aardig als die compliance officer terechte ethische vragen over zijn of haar werkzaamheden welbespraakt kan beantwoorden.
... Kortom, we hebben een moreel kompas nodig voor de digitale samenleving?
... Inderdaad, en dat zal er niet vanzelf komen. Aan de slag!

Leuk, een privacy officer, een PIA en een privacy statement, maar waar sta je als organisatie echt voor?

In deze boekenkast verdiep ik me in de digitale samenleving en ethische vragen die dit oproept. Steeds vaker worden die vragen aan mij gesteld: Edgar, wat vind jij van... Tsja, wat vind ik er van? De afgelopen jaren heb ik veel workshops gegeven, vaak aan verzekeraars, over *big data*, data analytics en privacy. Niet over de AVG. Die lost het probleem maar zeer ten dele op.[8] Maar over de morele uitdagingen die de nieuwe ontwikkelingen oproepen, uitdagingen die zich niet laten juridiseren. Leuk, een privacy officer, een PIA en een privacy statement, maar waar sta je als organisatie echt voor? 'We voldoen aan de wet' is een mooi begin, maar ook niet meer dan dat. Wat is het morele kompas van een financiële instelling? Dat leverde mooie gesprekken op, maar ook het inzicht dat dit weerbarstige materie is. Samen met het Verbond van Verzekeraars en het Koninklijk Actuarieel Genootschap hebben we een paper geschreven over de impact van de nieuwe technologische

[5] Kaplan, ibid.: 133.
[6] Segers, ibid.: 76.
[7] Segers, ibid.: 76.
[8] Vgl. WRR, *Big Data in een vrije en veilige samenleving*, Amsterdam University Press 2016.

ontwikkelingen op solidariteit in verzekeren.[9] In gesprek met pensioenfondsbestuurders bleek dat die discussie ook voor hen relevant is. Maar het zijn slechts deelterreinen. Hoe krijg je vat op het geheel, op de totaliteit aan ethische vragen die de digitale samenleving op ons afvuurt? Ik heb er de afgelopen tijd heel veel boeken over gelezen. Eerste conclusie: er zijn geen simpele antwoorden. Tweede conclusie: er zijn überhaupt nog maar heel weinig antwoorden, maar gelukkig wel denkrichtingen. Derde conclusie: het wordt hard werken.

'De digitale samenleving' is een heel breed begrip. Hiermee wordt naar een breed spectrum aan technologische gebieden verwezen: blockchain, The Internet of Things, biometrie, nudging, virtual reality, augmented reality, robotisering, kunstmatige intelligentie etc. etc. Mijn inzet is grip krijgen op de manier waarop we de dialoog over deze ontwikkelingen kunnen voeren, niet om de discussie te beslechten. Dat zou ook overmoedig zijn. Zo stelt Melanie Peters, directeur van het Rathenau Instituut, dat 'de overheid, de toezichthouders, het bedrijfsleven en de samenleving nog niet voldoende zijn toegerust om met deze nieuwe vragen om te gaan'.[10] En dat is zorgwekkend als we de digitalisering van de samenleving in goede banen willen leiden. We moeten dus eerst maar eens op zoek naar de woorden, de begrippen, de concepten en de dialoogvormen om de prangende vragen te stellen en mogelijke antwoorden te verkennen. Om deze bijdrage behapbaar te houden spits ik het toe op kunstmatige intelligentie (KI). Volgens Max Tegmark in *Life 3.0 Mens zijn in het tijdperk van kunstmatige intelligentie* is dat de belangrijkste discussie van onze tijd.[11] Kunstmatige intelligentie gaat een grote stap verder dan slechts gebruik maken van de enorme rekenkracht van computers. 'Anders dan gewone computerprogramma's, die van tevoren ingevoerde instructies opvolgen, ontdekt kunstmatige intelligentie zelfstandig verbanden tussen gegevens. Bovendien leert kunstmatige intelligentie zichzelf om daarin steeds beter te worden, en doet dit in een razendsnel tempo'.[12] KI kan hierdoor dingen doen die we tot voor kort alleen mensen zagen doen: 'Zo kan software (in beperkte mate) journalistieke bijdragen schrijven in domeinen als sport of de financiële beurzen. Watson, de slimme computer van IBM, wint taalspelletjes als Jeopardy! en als chef won hij in 2015 de Horecava Innovation Award. Software componeert ook symfonieën die experts niet van menselijke topcomponisten kunnen onderscheiden'.[13]

In paragraaf 2 bespreek ik een aantal zorgen die de digitale samenleving oproept en waarden die daarbij op het spel staan. Als gezegd: toegespitst op kunstmatige intelligentie. Ik beperk me hier nadrukkelijk tot de zorgen. In het dialoogje benoemde ik een groot aantal kansen en voordelen. Uiteindelijk zullen in de dialoog via een evenwichtig besluitvormingsproces alle kansen, risico's en zorgen moeten worden meegenomen. Een evenwichtig besluitvormingsproces zal niet gemakkelijk zijn. In paragraaf 3 benoem ik enkele valkuilen: naïef optimisme, neerslachtig pessimisme, puur instrumentalisme en technologisch determinisme. Hoe kun je om deze valkuilen heenlopen, hoe geef je vorm aan een evenwichtige belangenafweging? In paragraaf 4 bespreek ik het voorstel van Wright, om in navolging van een *privacy impact assessment* ook een *ethical impact assessment* te ontwikkelen. Hierbij worden enkele 'tools' gegeven om de dialoog hanteerbaar te maken. Ik rond af met de zorgplicht die ook financiële instellingen hebben ten aanzien van de discussie over de ethiek van techniek. Deze zorgplicht reikt verder dan handelen in het belang van de klant.

2. Maatschappelijke waarden op het spel

Wat zijn de zorgen die de digitale samenleving oproept en waarden die daarbij op het spel staan? Werkgelegenheid, zeker, dat staat op de kaart.[14] Net zoals privacy (gegevensbescherming, digitaal huisrecht, mentale privacy, surveillance, doelverschuiving) en veiligheid (informatieveiligheid, identiteitsfraude, fysieke veiligheid) ook al redelijk goed op de kaart staan.[15] Maar waar moeten we nog meer aan denken? Wat zijn andere zorgen die ontwikkelingen op het gebied van kunstmatige intelligentie oproepen? Welke andere waarden staan er op het spel? Ik bespreek zorgen rondom autonomie, menselijke waardigheid, rechtvaardigheid, solidariteit, controle over technologie en machtsverhoudingen. Ik maak hierbij vooral gebruik van het rapport *Opwaarderen. Borgen van publieke waarden in de digitale samenleving* van het Rathenau Instituut. Dit instituut stimuleert de publieke en politieke meningsvorming over de maatschappelijke aspecten van wetenschap en technologie. Het rapport laat zien 'hoe de verregaande digitalisering van de samenleving fundamentele ethische en maatschappelijke vragen oproept. ... Daardoor komen belangrijke publieke waarden en mensenrechten als privacy, gelijke behandeling, autonomie en menselijke waardigheid onder druk te staan'.[16] Ondanks alle zorgen heeft het rapport een optimistische ondertoon: 'we staan niet machteloos, met de juiste acties vanuit overheid, bedrijfsleven en maatschappij, kunnen we de digitale samenleving een verantwoorde opwaardering geven'.[17] Als we het goed

[9] Ton de Bruin en Edgar Karssing, *Verzekeren, technische solidariteit en morele solidariteit. Kiezen tussen de-solidarisatie en reddingsoperatie*, www.verzekeraars.nl/media/4072/verzekeren-technische-solidariteit-en-morele-solidariteit-11-oktober-2017.pdf. Zie voor een interview met mij hierover: https://www.verzekeraars.nl/publicaties/longreads/edgar-karssing-over-solidariteit (2017).

[10] M. Peters, 'Voorwoord' in Kool e.a., ibid.: 6.

[11] M. Tegmark, *Life 3.0 Mens zijn in het tijdperk van kunstmatige intelligentie*, Maven 2017: 58.

[12] B. de Wit, *Aan de vooravond van een maatschappelijke revolutie...*, oratie 5 april 2017, Nyenrode Business Universiteit 2017: 16.

[13] Kool e.a., ibid.: 39.

[14] Zie bijv. R. Went, M. Kremer, A. Knottnerus (red.), *De robot de baas. De toekomst van werk in het tweede machinetijdperk*. Amsterdam University Press 2015.

[15] Kool e.a., ibid.: 131.

[16] Kool e.a., ibid.: 6.

[17] Kool e.a., ibid.: 7.

doen, zou Nederland zelfs een gidsland kunnen worden en daarmee kansen kunnen creëren voor het Nederlandse bedrijfsleven![18] In het rapport wordt eerst een selectie van technologiegebieden gemaakt en vervolgens wordt onderzocht hoe de nieuwe ontwikkelingen op gespannen voet kunnen komen te staan met ethische waarden.[19] 'De verschillende ethische en maatschappelijke kwesties manifesteren zich per technologisch gebied op verschillende manieren. Privacy krijgt bijvoorbeeld in de context van robotica een andere invulling dan in de context van virtual reality'.[20] Het rapport kijkt naar veel meer technologiegebieden, hieronder richt ik me, als aangegeven, op kunstmatige intelligentie.

Kohnstamm spreekt over digitale predestinatie, waarbij mensen niet meer kunnen ontsnappen aan het profiel dat over hen is opgesteld

Autonomie

Autonomie verwijst naar de keuzevrijheid van mensen en is een voorwaarde voor een ongehinderde ontwikkeling van de eigen identiteit. Tegenover autonomie staan bijvoorbeeld manipulatie en technologisch paternalisme. 'Van paternalisme is sprake als iemand beter meent te weten wat goed voor anderen is dan deze anderen zelf. Bij technologisch paternalisme wordt het paternalisme "gedelegeerd" aan technologie'.[21] KI bepaalt wat voor jou goed is! Hierdoor kun je bijvoorbeeld in een informatiebubbel terechtkomen, waarin je alleen suggesties voor nieuws, informatie en contacten krijgt die passen bij je voorgaande gedrag, keuzes en interesses.[22] En dat beperkt je mogelijkheden om je blik te verruimen, om jezelf te ontwikkelen. Kohnstamm, voormalig voorzitter van College bescherming persoonsgegevens, spreekt over digitale predestinatie, waarbij mensen niet meer kunnen ontsnappen aan het profiel dat over hen is opgesteld: 'Via algoritmen wordt een profiel van je gemaakt waar je geen benul van hebt, waar je geen invloed op kunt uitoefenen en waaraan ingrijpende maatschappelijke gevolgen verbonden kunnen zijn'.[23] Profileren kan ook tot *chilling effects* leiden, waarbij mensen hun gedrag aanpassen omdat ze het gevoel hebben dat ze in de gaten worden gehouden. Zo kunnen 'overheden met behulp van data het gedrag van burgers proberen bij te sturen. Het meest in het oog springende voorbeeld hiervan komt van de Chinese overheid, die van alle burgers een *citizen score* bijhoudt, die een rol speelt bij het bepalen of iemand in aanmerking komt voor bijvoorbeeld een lening, een visum of baan'.[24]

Menselijke waardigheid

'De gedachte dat ieder mens onvervreemdbare waardigheid bezit, geldt zowel nationaal als internationaal als een van de basale beginselen van de morele en juridische ordening'.[25] Uitgangspunt is daarbij de Kantiaanse gedachte dat ieder mens altijd ook als doel op zichzelf moet worden beschouwd, en nooit alleen als middel.[26] Zo verwijst de eerste zin van art. 1 Universele Verklaring van de Rechten van de Mens (UVRM) reeds naar menselijke waardigheid: 'alle mensen worden vrij en gelijk in waardigheid en rechten geboren'. Ieder mens heeft recht om mens te zijn, om als mens te worden behandeld. Gebruik van algoritmen en KI kan ervoor zorgen dat mensen niet meer als mens worden gezien, maar als onderdeel van een groep en ook als zodanig worden behandeld. 'When individuals are treated not as persons but as mere temporary aggregates of data processed at an industrial scale so as to optimise through algorithmic profiling, administrative, financial, educational, judicial, commercial and other interactions with them, they are arguably, not fully respected, neither in their dignity nor in their humanity'.[27] Tevens kan KI, als reeds besproken, tot werkloosheid leiden, terwijl veel mensen zin en betekenis in hun bestaan juist ontlenen aan hun werk. En voor de mensen die hun baan behouden kan KI gebruikt worden om hun inzet te optimaliseren: op dat tijdstip hebben we zoveel mensen nodig. Hierdoor hebben deze werknemers geen vaste werktijden meer, en zeker als ze pas op het laatste moment hun werkschema krijgen, kunnen ze niet of nauwelijks nog hun privéleven plannen: 'the software also condemns a large percentage of our children to grow up without routines'.[28]

Wellicht draagt KI bij aan onze welvaart, maar hoe gaat die worden verdeeld? Wie zijn de winnaars, wie zijn de verliezers?

---

[18] Kool e.a., ibid.: 15.
[19] De geselecteerde technologiegebieden zijn: Internet of Things, robotica, biometrie, persuasieve technologie ('nudging'), virtual & augmented reality, digitale platformen, big data, slimme algoritmen en kunstmatige intelligentie. De maatschappelijke en ethische waarden waarnaar wordt gekeken zijn: privacy, autonomie, veiligheid, controle over technologie, menselijke waardigheid, rechtvaardigheid en machtsverhoudingen.
[20] Kool e.a., ibid.: 47.
[21] Kool e.a., ibid.: 50.
[22] Kool e.a., ibid.: 9.
[23] Speech Jacob Kohnstamm ter gelegenheid van zijn ceremoniële afscheid van de Autoriteit Persoonsgegevens op 2 juni 2016.
[24] Kool e.a., ibid.: 73.
[25] K. van der Wal, 'Waardigheid', in: M. Becker e.a., *Lexicon van de ethiek*, Van Gorcum 2007: 354.
[26] Vgl. Ethics Advisory Group (2018), *Towards a digital ethics*, EDPS: 16.
[27] Ethics Advisory Group, ibid.: 17.
[28] C. O'Neil, *Weapons of math destruction. How big data increases inequality and threatens democracy*, Penguin Books 2016: 129.

Rechtvaardigheid

Gebruik van kunstmatige intelligentie kan leiden tot discriminatie, uitsluiting en stigmatisering. 'Zo blijken softwareprogramma's die rechters in de Verenigde Staten bijstaan door de kans te berekenen dat een verdachte opnieuw de fout in gaat, in sommige gevallen te discrimineren'.[29] En het probleem is veel breder. 'Mensen kunnen op basis van hun profiel toegang tot een lening worden ontzegd, een hogere prijs moeten betalen voor hetzelfde product, of worden aangemerkt als verdachte. Fouten in analyses en profilering kunnen grote consequenties voor individuen hebben en dat is niet wenselijk. Het is tevens zeer onwenselijk dat door profilering systematisch bepaalde groepen mensen worden benadeeld'.[30] De inzet van kunstmatige intelligentie roept ook verdelingsvraagstukken op. Wellicht draagt KI bij aan onze welvaart, maar hoe gaat die worden verdeeld? Wie zijn de winnaars, wie zijn de verliezers? En hoe compenseren we de verliezers? Hoe zorgen we ervoor dat ook zij hun kansen behouden op de arbeidsmarkt? En zelfs als het zo is dat de digitale revolutie haar eigen werkgelegenheid creëert, hebben de mensen die hun baan verliezen dan de juiste kennis en vaardigheden om die banen in te vullen?[31]

Als we niet ingrijpen, zal profielenkennis de groep steeds verder uit elkaar drijven

Solidariteit

Solidariteit wordt vaak geassocieerd met begrippen als verbondenheid en saamhorigheid.[32] Je helpt elkaar zonder dat er onmiddellijk een tegenprestatie tegenover staat. Je doet het voor elkaar en met elkaar. En een bijdrage voelt niet als een offer maar als een investering in het collectief. Door data analytics-toepassingen krijgen bijvoorbeeld verzekeraars beter inzicht in risicoprofielen. Hierdoor kunnen steeds meer subcategorieën worden onderscheiden. Komt hiermee de solidariteit onder druk te staan? Welke verzekeraar durft af te wijken van de statistieken? Staan er straks klanten langs de zijlijn? Of zijn de goede risico's straks terecht beter af dan nu en was solidariteit alleen maar een slecht excuus om onvoorzichtig te zijn en risico te nemen? In een mooie column zet Marjan Slob het probleem scherp neer: 'Kennis over risico's maakt dat we elkaar de maat gaan nemen … Heb jij aanleg voor hartproblemen? Vervelend voor je, maar wil je dan wel de roomboter laten staan alsjeblieft? Want als jij niet een beetje je best doet, neemt de kans toe dat jij een beroep moet doen op de gezamenlijke pot. En dan gaat mijn premie omhoog, omdat jij te belazerd bent om te zorgen dat je niet ziek wordt. Zo maakt kennis over risico's dat we elkaar de maat gaan nemen. Ongemerkt worden we elkaars politieagenten … Hoe arrangeer je dan de solidariteit tussen zieke en nog-niet-zieke mensen? Vraag mij niet hoe dat moet. Ik heb slechts een voorspelling: als we niet ingrijpen, zal profielenkennis de groep steeds verder uit elkaar drijven. Solidariteit heeft altijd baat gehad bij een zekere blindheid.[33]

Door (semi-)automatische besluitvormingsprocessen kunnen mensen buiten de boot vallen, terwijl het probleem wellicht eerder de software of de data is dan de persoon die wordt afgewezen

Controle over technologie

Als steeds meer beslissingen worden genomen door algoritmen, door KI, of tenminste in belangrijke mate hierdoor worden ondersteund, wie heeft er dan controle over en inzicht in die processen? Cathy O'Neil bespreekt in haar boek met de omineuze titel *Weapons of math destruction. How big data increases inequality and threatens democracy* vele voorbeelden waarbij belangrijke beslissingen worden genomen – de vervroegde vrijlating van gevangenen, het ontslag van grote groepen leraren, online advertisement, de ranking van scholen, het aannamebeleid van organisatie – op basis van algoritmen die niet of nauwelijks inzichtelijk zijn. Want bedrijfsgeheim. Of omdat eigenlijk niemand het begrijpt. Ze noemt algoritmen 'meningen ingebouwd in wiskunde'.[34] Want de aannames en de definitie van succes zijn allesbepalend, samen met de invoer van data – garbage in, garbage out. 'Computer says no'. Door (semi-)automatische besluitvormingsprocessen kunnen mensen buiten de boot vallen, terwijl het probleem wellicht eerder de software of de data is dan de persoon die wordt afgewezen. Dan vrezen we wellicht de wereld die Orwell beschreef in *1984* waarin mensen voortdurend in de gaten worden gehouden ('Big Brother is watching you'), maar kunnen we beter beducht zijn voor Kafkaëske toestanden, als in Kafka's boek *Het proces*, waarin de burger compleet machteloos staat tegenover ondoorgrondelijke en onbegrijpelijke besluitvormingsprocessen.[35] Omdat de gevolgen groot kunnen zijn – *weapons of math destruction* – knelt dit gebrek aan controle. In het Rathenau rapport wordt op hetzelfde probleem gewezen, in iets minder poëtische taal: 'Naarmate er meer processen aan

---

[29] Kool e.a., ibid.: 128.
[30] Kool e.a., ibid.: 76.
[31] Vgl Kaplan, ibid.
[32] Voor deze subparagraaf is gebruik gemaakt van Ton de Bruin en Edgar Karssing, ibid.
[33] M. Slob, 'Solidariteit in de zorg heeft baat bij een zekere blindheid', *Volkskrant*, 9 oktober; Zie bijv. ook *Grip op data. Green paper Big Data*, Verbond van Verzekeraars, https://www.verzekeraars.nl/media/1489/grip-op-data-green-paper-big-data.pdf (2017).
[34] O'Neil, ibid.: 21.
[35] Ontleend aan M. Becker, *Ethiek van de digitale media*, Boom Uitgevers 2015: 85.

computersystemen worden uitbesteed, wordt de vraag belangrijker hoe menselijke controle over dergelijke systemen kan worden ingericht. Het gaat immers om systemen die medische diagnoses stellen, adviseren en ondersteunen in de rechtspraak, of bij autonome wapentechnologie zelfs beslissingen nemen over leven of dood. Inzicht in de manier waarop deze systemen tot een bepaalde beslissing komen is cruciaal om deze besluiten te kunnen verantwoorden, en om fouten te signaleren en tegen te gaan, bijvoorbeeld wanneer een systeem een onjuiste medische diagnose stelt door een fout in de software of de data'.[36]

Machtsverhoudingen

Dicteren straks de grote bedrijven hoe we moeten leven, wat we mogen eten, hoeveel stappen we zetten, welke keuzes we maken?[37] Bepalen verzekeraars die nieuwe technologieën inzetten om risicogedrag terug te brengen – 'een kastje in de auto' – wat gewenst en ongewenst gedrag is?[38] Kunnen werkgevers het gedrag van hun medewerkers sturen met behulp van wearables? Dat zou nogal wat zijn. En dan moeten we niet vergeten dat op het moment dat we ons denken uitbesteden aan machines, we in feite het denken uitbesteden aan de organisaties die de machines beheren.[39] Software speelt ook een steeds belangrijkere rol in dagelijkse producten en diensten. 'Degene met de zeggenschap over die software kan in de programmatuur bepalen hoe ze wel of niet gebruikt kan worden'.[40] Er komt dus steeds meer macht te liggen bij bedrijven. En dat mechanisme wordt nog versterkt door het *winner-takes-all*-effect: 'WhatsApp bijvoorbeeld werkt alleen als er een groot netwerk van gebruikers op zit. Als zo'n app dan eenmaal de grootste is, is het haast onmogelijk om hiermee te concurreren'.[41] En door het *lock-in*-effect 'dat ontstaat wanneer gebruikers niet gemakkelijk genoeg van de ene naar de andere aanbieder kunnen overstappen'.[42] Er is daarnaast sprake van een *transparantieparadox*, waarbij consumenten en burgers steeds transparanter worden voor bedrijven en overheid, terwijl andersom consumenten en burgers niet of nauwelijks inzicht hebben in de manier waarop organisaties analyses toepassen.[43] Kortom, 'Big data, slimme algoritmen en AI zorgen voor verschuivingen in machtsverhoudingen in de relatie tussen bedrijven, overheden en burgers'.[44]

3. Op zoek naar een moreel kompas

De ontwikkelingen gaan snel in de digitaliserende samenleving. Behoeven deze nieuwe technieken een nieuw moreel kompas? Een ander moreel kompas? Een moreel kompas 2.0? En hoe ziet dat er dan uit? De nieuwe mogelijkheden roepen in ieder geval nieuwe vragen op. Vragen waarover we met elkaar in gesprek zouden moeten gaan. Er staat immers wat op het spel. Onze menselijke waardigheid. Onze mogelijkheden om in vrijheid vorm te geven aan ons eigen leven. De kwaliteit van onze samenleving. De bescherming van zwakkere partijen in een transitie die winnaars en verliezers zal opleveren.

Erik Brynjolfsson en Andre McAfee concluderen in hun boek *Het tweede machinetijdperk. Hoe de digitale revolutie ons leven zal veranderen* 'dat de diepgaande veranderingen door de digitale technologie veranderingen ten goede zullen zijn. Het tijdperk dat voor de deur staat, wordt niet alleen anders maar ook beter'.[45] Dat is een fijne gedachte. Nu ben ik van nature optimist. Ik geloof zelfs in een morele plicht tot optimisme, als verwoord door mijn held sir Karl Popper.[46] Maar het is niet moeilijk om je eigen pessimisme te voeden. In het dialoogje aan het begin van deze bijdrage kwamen optimisme en pessimisme beide al langs. Natuurlijk bieden de nieuwe ontwikkelingen enorme kansen, voor bedrijven, voor welvaart en welzijn. Maar er zijn zeker ook netelige problemen. Dat bleek wel in de vorige paragraaf. Genoeg voedingsbodem voor neerslachtig pessimisme. Brynjolfsson en McAfee onderkennen die netelige problemen ook. Maar met een optimistische inslag. 'De problemen die de digitale revolutie brengt, kunnen ook worden opgelost, maar dan moeten we wel eerst helder krijgen wat die problemen precies zijn. Het is daarom van groot belang dat we de eventuele negatieve gevolgen van het tweede machinetijdperk ter discussie stellen en een dialoog starten over mogelijke oplossingen. We hebben er alle vertrouwen in dat de problemen niet onoverkomelijk zullen blijken. Maar vanzelf overgaan zullen ze zeker niet'.[47] Een zelfde optimisme zie ik in het boek *Humans need not apply. A guide to wealth & work in the age of artificial intelligence* van Jerry Kaplan: 'Despite this litany of plagues, I remain an optimist. I'm confident we can craft a future of eternal peace and unbounded prosperity. In the end, the tsunami of new technology will sweep in an extraordinary era of freedom, convenience, and happiness, but it's going to be a rough ride if we don't keep our hands firmly on the wheel of progress'.[48] Kortom, er liggen kansen, maar we mogen de netelige kwesties niet veronachtzamen. We moeten de hand aan het

---

[36] Kool e.a., ibid.: 76.
[37] T. Schep, *Design my privacy. 8 principes voor beter privacy design*, BIS 2016: 12.
[38] J. Timmer e.a., *Berekende risico's: Verzekeren in de datagedreven samenleving*. Rathenau Instituut 2015.
[39] F. Foer, *Ontzielde wereld. De existentiële dreiging van big tech*, De bezige bij 2017: 92.
[40] Kool e.a., ibid.: 76.
[41] Kool e.a., ibid.: 68.
[42] Kool e.a., ibid.: 119.
[43] WRR, ibid.: 75.
[44] Kool e.a., ibid.: 73.
[45] Brynjolfsson en McAfee, ibid.: 18.
[46] 'The future is open ... When I say "It is our duty to remain optimists", this includes not only the openness of the future but also that which all of us can contribute to it by everything we do: we are all responsible for what the future holds in store. This is our duty, not to prophesy evil but, rather fight for a better world'. Geciteerd in: N. Koertge, *The moral underpinnings of Popper's philosophy*: 7. http://www.indiana.edu/~koertge/rCamb_Popper.pdf.
[47] Brynjolfsson en McAfee, ibid.: 19-20.
[48] Kaplan, ibid.: 16.

stuur houden en in dialoog samen zoeken naar de manier waarop we onze toekomst vorm willen geven. Dan ontstaat er ruimte voor bedachtzaam optimisme: 'Het gaat dan om de verwachting dat er iets goeds gebeurt als je daar hard je best voor doet en er doelgericht en met zorg naartoe werkt'.[49]

Je zet dan de ethiek voortijdig buiten spel, waarmee je je aan de techniek overgeeft. Dat is dan een *self-fulfilling* prophecy

Overigens, volgens sommigen valt er weinig vorm te geven. Ook dat standpunt zagen we al in het dialoogje: 'Joh, wat maak jij je druk. Alsof wij enig invloed hebben op de toekomst. De technologie gaat toch zijn eigen gang'. Dat is *technologisch determinisme*: 'technische ontwikkelingen hebben een eigen dynamiek waar de mens geen macht over heeft'.[50] De tegenhanger is het *instrumentalisme*: mensen kunnen geheel naar eigen inzicht techniek inzetten. Of niet. Voor de dialoog maakt het nogal uit welk standpunt je inneemt. Want in een wereld van technologisch determinisme heeft de dialoog weinig zin: wat gebeurt, gebeurt. De ethische dimensie raken we dan kwijt. De techniek gaat zijn geheel eigen gang, heeft een eigen dynamiek en daar hebben wij mensen weinig invloed op. En dan heeft het dus weinig zin om je er druk over te maken. Omarm met vreugde of accepteer gelaten. Dat zijn de twee keuzes die overblijven. Het determinisme heeft dus een verlammend effect op ethische discussies.[51] Marcel Becker noemt dat in *Ethiek van de digitale media* ethische luiheid. Mijns inziens terecht. Je zet dan de ethiek voortijdig buiten spel, waarmee je je aan de techniek overgeeft. Dat is dan een *self-fulfilling prophecy*: dan gebeurt inderdaad wat gebeurt.[52] Volgens het instrumentalisme staat de mens aan het roer en bepalen we zelf of we techniek ten goede of ten kwade inzetten. En met die handelingsvrijheid komt verantwoordelijkheid. Maar een puur instrumentalisme is naïef. De techniek bepaalt mede ons denken doordat ze alomtegenwoordig is: 'Digitalisering dringt door tot ieder aspect van ons leven: technologie nestelt zich *in* ons (bijvoorbeeld via hersenimplantaten), *tussen* ons (via sociale media als Facebook), weet steeds meer *over* ons (via big data en technieken als emotieherkenning), en weet zich steeds beter te gedragen *als* ons (robots en software vertonen intelligent gedrag en kunnen emoties nabootsen)'.[53] En op heel veel ontwikkelingen hebben we geen of nauwelijks invloed. We zullen dus ergens een middenweg moeten nemen tussen technologisch determinisme en puur instrumentalisme. Dus niet alleen maar fantaseren over wat er allemaal gaat gebeuren. Tegmark formuleert het scherp: 'In mijn ogen is het een vraag die ons op het verkeerde been zet. Het zou een vergissing zijn om ons passief af te vragen 'Wat er zal gebeuren?" alsof de toekomst al vastligt... De vraag die we onszelf moeten stellen is dan ook deze: "Wat zou er moeten gebeuren? Wat voor toekomst willen we hebben?"... Pas wanneer we serieus hebben nagedacht over wat voor toekomst we willen, zullen we in staat zijn een koers te bepalen voor de toekomst die we ons wensen. Als we niet weten wat we willen, is de kans klein dat we die ook krijgen'.[54] We moeten dus de hand aan het stuur houden en in dialoog samen zoeken naar de manier waarop we onze toekomst vorm willen geven, waarbij we waken voor ethische luiheid en naïviteit.

Pas wanneer we serieus hebben nagedacht over wat voor toekomst we willen, zullen we in staat zijn een koers te bepalen voor de toekomst die we ons wensen

En dan nog zal het niet gemakkelijk gaan. Olga Crapels heeft met *Morele democratisering van publieke debatten over nieuwe technologie* een zeer leesbaar proefschrift geschreven over publieke debatten over technologische ontwikkelingen. In haar proefschrift spitst ze zich toe op genomics, op biotechnologische innovaties met genen. Ze constateert dat veel van deze discussies weinig opschieten: er is een nieuwe ontwikkeling, dit roept vragen op, vragen die vaak gaan over waar onze grenzen liggen, of alles mag wat kan. Er wordt van alles geroepen, er wordt nauwelijks geluisterd en er is weinig overeenstemming. De commotie en daarmee het debat ebt vervolgens weg totdat er een nieuwe doorbraak in de krant staat en het debat van voor af aan begint, dezelfde posities worden ingenomen en geen vooruitgang wordt geboekt. Dat lijkt me een schrikbeeld voor de dialoog over de digitaliserende samenleving. Om een dergelijke herhaling van zetten te voorkomen formuleert Crapels een aantal voorwaarden waaraan de dialoog moet voldoen, waaronder redelijkheid en inclusiviteit. 'Daarmee wordt bedoeld dat vragen en argumenten begrijpelijk en navolgbaar zijn voor andere deelnemers aan het debat, dat alle serieuze vragen en argumenten kunnen worden ingebracht, dat iedereen aan het debat kan deelnemen, en dat debatten publiek toegankelijk zijn'.[55] Maar dat is nog niet voldoende. Er is ook intellectuele moed nodig: 'Door je in te graven achter een morele positie, wordt de mogelijkheid uitgesloten om te twijfelen, de eigen opvattingen kritisch te bevragen en om je te laten overtuigen door

---

[49] Tegmark, ibid.: 472.
[50] Becker, ibid.: 19.
[51] Becker, ibid.: 23.
[52] Becker, ibid.: 24.
[53] Kool e.a., ibid.: 30.
[54] Tegmark, ibid.: 229.
[55] O. Crapels, *Morele democratisering van publieke debatten over nieuwe technologie*, proefschrift, Universiteit Leiden 2012: 161.

de kracht van het betere argument. ... Intellectueel moedig zijn vereist de bereidheid om de eigen overtuigingen aan te passen, met het gevaar dat het beeld dat je van jezelf hebt, of dat anderen van je hebben, verandert'.[56] Moedig voorwaarts!

4. Een ethical impact assessment

De hand aan het stuur houden en in dialoog samen zoeken naar de manier waarop we onze toekomst vorm willen geven. Dat is de opdracht. Hoe kun je dat oppakken? Als compliance officer? In zijn artikel *A framework for the ethical impact assessment of information technology* bepleit David Wright een gestructureerde en systematische aanpak van de ethische vragen die nieuwe technologieën oproepen.[57] Hij noemt dit een 'ethical impact assessment' (EIA). Het aantrekkelijke van zijn voorstel is dat dit voor compliance officers geen wezensvreemde aanpak is, maar eigenlijk voortbouwt op een PIA, een privacy impact assessment.[58] Om even op te frissen, een PIA 'legt in de eerste plaats de privacyrisico's bloot van nieuwe (projecten en initiatieven) of bestaande verwerkingen van persoonsgegevens en draagt bij aan het vermijden of verminderen van deze privacyrisico's. Op basis van deze PIA wordt op systematische wijze inzichtelijk gemaakt hoe groot de kans is dat de privacy van de betrokken personen van wie gegevens worden verwerkt wordt geschaad, waar deze risico's zich voordoen en welke gevolgen daaraan voor hen verbonden zijn. De PIA doet dit door op gestructureerde wijze:

- de mogelijk (negatieve) gevolgen van het gebruik van persoonsgegevens voor de betrokken personen en organisaties in kaart te brengen; en
- de risico's voor de betrokken personen en organisaties zo veel mogelijk te lokaliseren.

Op basis van de uitkomsten van de PIA kunt u gericht acties ondernemen om deze risico's te verminderen'.[59]

Je zou kunnen stellen dat een PIA naar een deel kijkt (privacy) en een EIA naar het geheel aan ethische aspecten van nieuwe technologieën. Het is een manier 'to ensure ethical implications are adequately examined by stakeholders before deployment and so that mitigating measures can be taken as necessary'.[60] Dat is zeker verstandig bij het ontwikkelen van nieuwe producten en diensten, in een adequaat productontwikkelingsproces. Maar omdat de ontwikkelingen momenteel op de reflectie vooruitlopen, lijkt het me niet onverstandig om ook bestaande producten en diensten (van de eigen organisatie, maar wellicht zelfs van klanten) aan een EIA te onderwerpen. En dan kijk je dus verder dan de KNVB-norm van de AFM: kostenefficiëntie, nut, veiligheid en begrijpelijkheid. Want dat beperkt zich tot het perspectief van de klant. Zeker belangrijk, maar er staat nu meer op het spel.

Door stakeholders bij de discussie te betrekken verklein je ook het risico dat een nieuw product 'ontploft' doordat het onverwacht enorme weerstand oproept

Een EIA doe je bij voorkeur niet alleen. Volgens Wright is het zelfs een belangrijk doel van een EIA om stakeholders hierbij te betrekken om op die manier ethische aspecten van nieuwe technologieën te identificeren, te articuleren en te bespreken.[61] Ook kunnen stakeholders met oplossingen komen (waarborgen) waar je zelf wellicht nog helemaal niet aan had gedacht. Door stakeholders bij de discussie te betrekken verklein je ook het risico dat een nieuw product 'ontploft' doordat het onverwacht (want niet op voorbereid) enorme weerstand oproept. Juist door stakeholders te betrekken bouw je ook goodwill bij hen op. Op deze manier is een EIA dus zowel een 'early warning system' als een manier om advies te krijgen.[62]

> 'While it may be impossible to foresee all of the ethical and other consequences of an emerging technology, nevertheless, an ethical impact assessment, involving different stakeholders from different disciplines and backgrounds, may be a good way of avoiding the traps ... of not seeing the context specificity of a technology and of not examining its critical implications for individuals, groups, organisations and society'.[63]

Wright bespreekt twee verschillende soorten instrumenten om invulling te geven aan een EIA: inhoudelijk en procedureel. Een meer inhoudelijke instrument is bijvoorbeeld een handreiking met mogelijk relevante waarden, een opsomming van mogelijk relevante stakeholders en een overzicht van vragen die gesteld kunnen worden over de impact van het product of de dienst. Het zijn handreikingen om direct aan de slag te gaan met de inhoud. Bij bijvoorbeeld de waarde 'rechtvaardigheid' formuleert hij de volgende vragen:

---

[56] Crapels, ibid.: 163.
[57] D. Wright, 'A framework for the ethical impact assessment of information technology', *Ethics and Information Technology* 2011, Vol. 13 Iss. 3, p. 199-226.
[58] En bijvoorbeeld ook nauw verwant is aan een Human Rights Impact Assessment. Zie www.amnesty.nl/encyclopedie/human-rights-impact-assement.
[59] NOREA (2015), *Privacy Impact Assessment (PIA). Introductie, handreiking en vragenlijst*, https://www.norea.nl/, zie ook https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacycheck.
[60] Wright, ibid.: 199.
[61] Wright, ibid.: 200.
[62] Wright, ibid.: 202.
[63] Wright, ibid.: 203.

- 'Has the project identified all vulnerable groups that may be affected by its undertaking?
- Is the project equitable in its treatment of all groups in society? If not, how could it be made more equitable?
- Does the project confer benefits on some groups but not on others? If so, how is it justified in doing so?
- Do some groups have to pay more than other groups for the same service?
- Is there a fair and just system for addressing project or technology failures with appropriate compensation to affected stakeholders?'.[64]

Doordat je met waarden begint, heb je meteen een eerste kader voor het beoordelen van antwoorden (draagt dit bij aan... staat dit op gespannen voet met...). Je begint met een aantal waarden en geeft aan welke vragen deze oproepen. Daarbij wordt niet gestreefd naar een uitputtende opsomming van mogelijke vragen, het zijn startpunten voor het goede gesprek. Ook een *ethische matrix* kan een handvat bieden voor reflectie. Hiermee kunnen de belangrijkste waarden en stakeholders in kaart worden gebracht. Net als met een checklist met de belangrijkste vragen. Zo werkt dat bijvoorbeeld ook met een PIA. Gevaar is dat na een aantal keren het vooral een invuloefening wordt. Ook is het niet mogelijk om op voorhand alle relevante aspecten in kaart te brengen. 'The checklist can, however, make sure that ethical issues that are foreseeable are indeed identified. The checklist is only a tool to quickly identify ethical issues. If ethical issues are identified then a thorough ethical analysis should be made'.[65]

De meer procedurele instrumenten om vorm te geven aan een EIA zijn 'ethical tools' om de dialoog mee te organiseren. Wellicht kan één gek meer vragen stellen dan 1000 wijzen kunnen beantwoorden... maar het is toch wel prettig om ook werkvormen te hebben om toch een poging te wagen. De 'tools' ondersteunen een gestructureerde en systematische reflectie op nieuwe technologieën en ondersteunen het gesprek over waarden. Het zijn hulpmiddelen, om in de sfeer te blijven, geen algoritmen om tot de juiste conclusies te komen. Het nadenken, het oordelen moet je nog steeds zelf doen. Wright biedt een hele gereedschapskist, vanuit de gedachte dat meerdere 'tools' tegelijkertijd nodig zijn en de inzetbaarheid van een bepaalde werkvorm mede afhankelijk is van de context en de mogelijkheden die deze biedt. Een belangrijk uitgangspunt is inclusiviteit: probeer zoveel mogelijk verschillende geluiden aan tafel te krijgen.

Ik noem kort verschillende 'ethical tools'. Dit is niet de plaats om ze uitgebreid uit te werken, om ze van een handleiding te voorzien. Wel kan al iets worden gezegd over de voor- en nadelen van de verschillende 'tools'. Een manier om meningen, opinies en inzichten te inventariseren is een *vragenlijst*. Voordeel hiervan is dat deze onder grote groepen kan worden uitgezet, nadeel is dat de respons vaak laag is en dat er weinig ruimte is voor nuances, uitweidingen en mijmeringen. Dit kan worden ondervangen door een paper 'ter *consultatie*' aan te bieden waarop men uitgebreid kan reageren. Maar ook dan is de respons vaak laag en het gevaar bestaat dat vooral 'belangengroepen' reageren.[66] Als alternatief, of aanvulling, kun je expert-meetings organiseren, waarbij bijvoorbeeld presentaties van experts worden afgewisseld met diepgravende inhoudelijke discussies. Het resultaat kan een rapportage zijn waarop eventueel andere experts en/of stakeholders kunnen reageren. Aanvullend of als alternatief is er de Delphi-methode. Hierbij wordt de meningen van een groot aantal experts gevraagd. Door de antwoorden van de andere experts (anoniem) terug te koppelen wordt in een aantal rondes geprobeerd meer inzicht te verkrijgen. 'The ethical Delphi is used to map the ethical considerations that experts believe are pertinent and significant. It indicates the extent of agreement as well as drawing out divergence in expert opinion on a given topic'.[67] Daarnaast kun je ook consumentenpanels (of burgerpanels) organiseren om breed inzicht in de thematiek te krijgen.

Een EIA is een hulpmiddel om beter inzicht te krijgen in de problematiek, de verantwoordelijkheden die men bereid is te accepteren en een invulling en uitwerking van het eigen morele kompas

Het organiseren van dergelijke dialogen is natuurlijk spannend. Je weet op voorhand niet wat er gaat gebeuren, wie wat inbrengt, en of er enige mate van consensus kan worden bereikt. Dat laatste zou ook niet per se het doel moeten zijn. Een EIA is een hulpmiddel om beter inzicht te krijgen in de problematiek, de verantwoordelijkheden die men bereid is te accepteren en een invulling en uitwerking van het eigen morele kompas. Een belangrijk onderdeel van een evenwichtig besluitvormingsproces waarin alle kansen, risico's en zorgen worden meegenomen. Dan is het verstandig van een financiële instelling om zich breed te oriënteren, het is nog iets anders om de zeggenschap over het eigen morele kompas uit handen te geven. Het is wel zo netjes om de deelnemers achteraf te informeren over de keuzes die zijn gemaakt en waarom. Voordeel van een goede dialoog is dat die reeds de argumenten heeft opgeleverd om dit onder woorden te brengen.

[64] Wright, ibid.: 210.
[65] Wright, ibid.: 217.
[66] Wright, ibid.: 216.
[67] Wright, ibid.: 218.

5. Conclusie: een morele zorgplicht

'The new digital age generates new ethical questions about what it means to be human in relation to data, about human knowledge and about the nature of human experience. It obliges us to re-examine how we live and work and how we socialise and participate in communities. It touches our relations with others and perhaps most importantly, with ourselves. If we accept the idea of a new digital reality, we also accept that it brings with it changing conditions of being human. It invites a new ethical evaluation, a new interpretation of some of the fundamental notions in ethics, such as dignity, freedom, autonomy, solidarity, equality, justice, and trust; and invites us to test the conditions of their validity for the new realities that present themselves in this new age'.[68]

Er zijn allemaal processen gaande, heel lang zie je niks, en opeens... zo gaat het ook met de digitaliserende samenleving. De melk kookt. Of in ieder geval bijna

... De melk kookt!
... Huh?
... Dat was een uitdrukking van de onlangs overleden Ruud Lubbers. 'Je kunt het beeld gebruiken van een pannetje melk. De temperatuur lijkt niks te veranderen, maar op een gegeven moment gaat het opeens koken en dan zeg je "Hé, het kookt"'. Hij had het over globalisering.[69] Er zijn allemaal processen gaande, heel lang zie je niks, en opeens... zo gaat het ook met de digitaliserende samenleving. De melk kookt. Of in ieder geval bijna.
... Tsja. En ik vind privacy al zo'n gedoe.
... Het goede nieuws is dat we kunnen voortbouwen op onze ervaringen met dat thema. We hoeven niet helemaal vanuit het niets te beginnen.
... En we kunnen dus niet onze kop in het zand steken?
... Volgens het Rathenau Instituut is het tijd om de fundamentele impact van digitalisering op de samenleving te onderkennen en ervoor te zorgen dat publieke waarden en grondrechten in het digitale tijdperk worden geborgd.[70]
... En daar moeten wij aan meedoen?
... Daar moet iedereen aan meedoen. Melanie Peters benadrukt ook de zorgplicht van bedrijven: 'zet de zorgplicht centraal om rekening te houden met maatschappelijke en ethische vraagstukken van digitale producten en diensten'.[71] En terecht. With great power comes great responsibility! En die zorgplicht reikt dus veel verder dan het belang van de klant centraal stellen. Zoals in steeds meer codes van financiële instellingen wordt aangegeven, het gaat hier om 'society at large'.
... Wie gaat ons helpen?
... Laten we beginnen met de vinger aan de pols te houden. Zo houdt het Verbond van Verzekeraars met een solidariteitsmonitor in de gaten of verzekerden in de toekomst niet meer worden geaccepteerd of alleen tegen zeer hoge premies.[72]
... En verder?

With great power comes great responsibility! En die zorgplicht reikt dus veel verder dan het belang van de klant centraal stellen

... Op Europees niveau heeft bijvoorbeeld Mady Delvaux de discussie aangezwengeld. Met een advies aan de Europese Commissie pleit ze voor het reguleren van robots en kunstmatige intelligentie.[73]
... Zeker een saai stuk?
... Ze begint heel frivool: 'from Mary Shelley's Frankenstein's Monster to the classical myth of Pygmalion, through the story of Prague's Golem to the robot of Karel Čapek, who coined the word, people have fantasised about the possibility of building intelligent machines, more often than not androids with human features'. En daarna volgt een heel gedegen analyse. Ook zij benoemt een groot aantal zorgen en waarden. Een inspirerend stuk.
... Dus door enig leeswerk kunnen we snel grote stappen zetten!
... Interessant is ook het rapport *Towards a digital ethics* van de Europese privacytoezichthouder.[74] Ook hierin wordt een groot aantal zorgen en waarden benoemd en geven de auteurs nadrukkelijk aan dat de discussie voortbouwt op de discussie over privacy. Verder denk ik dat het ook helpt om scenario's in kaart te brengen, om onze fantasie te prikkelen.
... Oh, dan moet je *Homo Deus* eens lezen, van Yuval Noah Harari. Fascinerend, maar wel wat deprimerend.
... Inderdaad, fascinerend. En bijvoorbeeld Tegmark werkt in zijn *Life 3.0* ook een groot aantal scenario's uit. Goed om er kennis van te nemen. En met elkaar te onderzoeken hoe we onze toekomst vorm willen geven. Wie weet ontdekken we dan wel heel nieuwe waarden. Zo bepleit het Rathenau Instituut het recht om niet gesurveilleerd of heimelijk beïnvloed

---

[68] Ethics Advisory Group, ibid.: 15.
[69] E. Karssing, 'De melk kookt! Interview met Ruud Lubbers', *Filosofie in bedrijf: tijdschrift voor strategie en organisatie* 1999, nr. 2, nr. 33, p. 28-35.
[70] Zie bijv. ook De Wit, ibid.
[71] Kool e.a., ibid.: 15.
[72] https://www.verzekeraars.nl/publicaties/actueel/verbond-lanceert-eerste-solidariteitsmonitor.
[73] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//EN.
[74] Ethics Advisory Group, ibid. zie ook: European Group on ethics in science and new technologies (maart 2018), *Statement on Artificial Intelligence, robotics and 'autonomous' systems*: ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

te worden en het recht op betekenisvol menselijk contact.[75]

... En we kunnen dus aan de slag met *ethical impact assessments*.

... Precies, zoals het Rathenau Instituut dat in meer algemene zin heeft gedaan, kunnen wij voor onze eigen situatie onze eigen analyse maken. Met een EIA, voor een redelijke, inclusieve en intellectueel moedige dialoog over de digitale samenleving. ■

[75] R. van Est e.a., *Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality*, Rathenau Instituut 2017.