POLITIE
Midden Nederland

Bestuurlijk Dossier:

Misbruik van prepaid telefoons bij misdrijven

Dossier	:	Misbruik van prepaid telefoons bij misdrijven
Rapporteur	:	[redacted] adviseur Tegenhouden Politie Midden Nederland, Dienst Regionale Recherche
Opdrachtgever	:	MT van BR-Midden-Nederland, in samenspraak met adviseurs van het Team Tegenhouden
Status	:	Definitief
Ten behoeve van	:	Ministerie van Veiligheid & Justitie, Ministerie van Economische zaken, Telecom aanbieders,
Datum rapport	:	19 november 2013
Bijlagen	:	Drie

Managementsamenvatting

N.B. Daar waar in dit bestuurlijke dossier wordt gesproken over een prepaid telefoon, wordt bedoeld: een niet geregistreerde telefoon in combinatie met een niet geregistreerde simkaart. Met andere woorden: Het Imeinummer van de telefoon is onbekend en is niet gekoppeld aan een persoon en het 06 nummer van de simkaart is niet op naam geregistreerd.

Aanleiding

In 2012 kwamen bij de Bovenregionale Recherche (Midden-Nederland) 25 aangiften- en 36 meldingen binnen van diefstal uit woning dmv een bepaalde babbeltruc. De babbeltruc kent vele variaties, maar in de genoemde aangiften en meldingen was niet alleen de "babbel" hetzelfde, maar ook het gebruikte middel: een niet geregistreerde prepaid telefoon. Door het gebruik (misbruik) van dergelijke "anonieme" prepaid telefoons, was de dader niet te achterhalen. Dit "fenomeen", waar rechercheurs in allerlei opsporingsonderzoeken mee te maken krijgen, was aanleiding voor bureau Tegenhouden, om onderzoek te doen naar dit fenomeen en naar een oplossing te zoeken.

Voortschrijdend inzicht

Een verdachte met een niet geregistreerde prepaid telefoon is niet iets waar alarmbellen van gaan rinkelen. Maar als blijkt dat vrijwel alle verdachten gebruik maken van zo'n

anoniem communicatiemiddel, zet dit wel aan tot nadenken. Tijdens het onderzoek naar dit fenomeen bleek dat bijna iedere aangehouden verdachte (85%) in het bezit bleek te zijn en gebruik maakte van een niet geregistreerde prepaid telefoon. Dit geldt trouwens niet alleen bij woninginbraken (babbeltruc), maar voor alle soorten misdrijven. Wat deze constatering in de praktijk betekent, wordt in dit dossier uitgelegd en duidelijk gemaakt.

Ernst en omvang van het probleem (fenomeen)

Het probleem is veel meer omvattend dan gedacht. Niet geregistreerde prepaid telefoons worden veel gebruikt bij het plegen van misdrijven. Denk hierbij niet alleen aan mensenhandel, heling, vuurwapen- en drugscriminaliteit, inbraken, babbeltruc, fraude, afpersing en afdreiging, maar ook aan het beramen van terroristische acties. Bij gebruik van niet geregistreerde prepaid telefoons blijft de beller anoniem. Logisch dat criminelen dit middel hebben omarmd. Er zijn voldoende politieonderzoeken waaruit blijkt dat anonimiteit aan criminaliteit gekoppeld kan worden. Om diezelfde reden gebruiken criminelen ook valse (gekopieerde) kentekenplaten.

Niet alleen criminelen maken gebruik van deze "anonimiteit". Ook jongeren die elkaar anoniem telefonisch pesten, dreig-tweets sturen, valse 112 meldingen doen, opruiing plegen (project-X) etc, maken hier gebruik van.

In 2011 werden volgens het CBS 1,2 miljoen (1.192.755) misdrijven geregistreerd. In 2012 registreerde de politie 1,14 miljoen misdrijven, 5 procent minder dan in 2011. Daarvoor werden 372.305 verdachten aangehouden. Uit de politiesystemen (fouilleringlijsten, historie printgegevens en Digitale Communicatie Sporen) is op te maken dat gemiddeld 85 % van alle terzake misdrijf aangehouden verdachten gebruik maakt(e) van een niet geregistreerde prepaid telefoon. Uit cijfers van de Opta blijkt dat er in 2011 meer dan 6,2 miljoen prepaid telefoons in Nederland in gebruik waren. Cijfers over 2012 zijn nog niet bekend.

Prepaid aanschaffen

Bij supermarkten en warenhuizen zoals [redacted] etc zijn prepaid telefoons- en simkaarten volop te koop. Deze telefoons met simkaart worden zonder enige vorm van registratie verkocht. Soms met tientallen per klant tegelijk. De reden om niet te hoeven registreren is puur economisch en voor het gemak. Op de kassabon wordt alleen het artikelnummer geprint en dat nummer is voor alle telefoons in die winkel hetzelfde. Geen contract, geen registratie en geen kredietcheck.

Aanpak in het buitenland

Niet alleen in Duitsland, Italië, Zwitserland, Hongarije, Japan, Turkije, de meeste Afrikaanse landen, maar ook in Dubai en Singapore is het verboden om een prepaid telefoon aan te schaffen zonder dat men zich registreert. In Kenia is het zelfs verboden een niet geregistreerde telefoon bij je hebben. Overweging van de regeringen was puur het tegengaan van criminaliteit en het beter kunnen voorkomen/bestrijden van terroristische acties. Het effect daarvan is merkbaar geweest bij de in 2013 gehouden (vreedzaam verlopen) verkiezingen in Kenia. Hoe e.e.a. in Duitsland is geregeld kunt u lezen op pagina 14.

Maatschappelijke relevantie

[redacted] In de vorige alinea werd duidelijk gemaakt dat andere landen het prepaid bellen verbieden om misdaad en terroristische acties tegen te gaan. Hoewel de kans in Nederland niet groot is op een terroristische actie, is het dreigingsbeeld wel reëel. Een terroristische actie kent enorme psychische- en economische (gevolg)schade. Niet alleen bij de burger, maar ook bij bancaire- en particuliere instellingen en overheidsdiensten. Uiteindelijk kan dit leiden tot schade aan het (internationale) imago van Nederland.

Conclusie

- Het bezit van een niet geregistreerde prepaid telefoon en de daaruit voortvloeiende anonimiteit, lijkt anno 2013 bij veel criminelen te voldoen als een basisbehoefte voor het plegen van misdrijven.
- Het fenomeen van het anoniem bellen met een prepaid telefoon is volledig geaccepteerd in de maatschappij en de "onwetende" burger is zich niet bewust van de negatieve criminele aspecten.
- [redacted]
- Tijdens dit onderzoek is, buiten het advies uit politieonderzoek "Apollo" (pag.22), nergens uit gebleken of er in Nederland is nagedacht over een strategie of maatregel om dit fenomeen te stoppen cq tegen te houden.

Doel van dit dossier

1. Met dit bestuurlijke dossier worden betrokken partijen ingelicht en bewust gemaakt van de ernst en omvang van dit fenomeen. De zo onschuldig lijkende verkoop van anonieme telefoons is blijkbaar een basisbehoefte voor het plegen van misdrijven.
2. [redacted]

Adviezen

Alle betrokken partijen dienen hun systemen en procedures op de genoemde adviezen aan te passen en actief te participeren.

1 [redacted]

Randvoorwaarden

[redacted]

Het spreekt voor zich om de genoemde partners in dit traject te betrekken, zodat de noodzakelijke regelgeving volledig aansluit bij de uitwerking door de sector. Hiermee kan onnodig belastende regelgeving voor alle betrokken partners worden voorkomen.

Het dossier

In het dossier wordt dieper ingegaan op het fenomeen van het misbruik van de niet geregistreerde prepaid telefoon. Alle voor- en tegens worden nader beschouwd. Het begrip 'registratie' wordt uitgebreid behandeld. Ook wordt stil gestaan bij de bepalingen ten aanzien van de privacy wetgeving; de vrijheid van meningsuiting (art 8 EVRM), de schending van het recht op anonieme communicatie en de maatschappelijke relevantie. Verder wordt een afweging gemaakt tussen het faciliteren van dit fenomeen (economische belang) en de gevolgen daarvan op de maatschappij (criminaliteit).

Inhoudsopgave pag.

LEESWIJZER

Na de inleiding in hoofdstuk 1, waarin de lezer bekend wordt gemaakt met de inhoud van de casus en de reden voor dit dossier, komt in hoofdstuk 2 de omschrijving van het probleem aan bod.

In hoofdstuk 3 wordt de doelstelling en het beoogde effect behandeld.

In hoofdstuk 4 komt naar voren hoe men in het buitenland omgaat met dit probleem (misbruik van niet-geregistreerde prepaid telefoons) en wordt een koppeling gelegd met terrorisme.

In het vijfde hoofdstuk wordt duidelijk op welke wijze prepaids kunnen worden aangeschaft en wat de omvang is van het probleem.

In hoofdstuk 6 wordt de maatschappelijke relevantie besproken en de(strafrechtelijke) betrokkenheid van de partners.

Hoofdstuk 7 beschrijft de uitkomst van het in 2008 gehouden onderzoek "Apollo" door de BR's uit Haarlem, Den Haag, Rotterdam en Amsterdam.

Hoofdstuk 8 is grotendeels gewijd aan de bezwaren rondom de vrijheid van meningsuiting en de reactie van het College Bescherming Persoonsgegevens.

Tot slot zullen in hoofdstuk 9 en 10 de conclusies en aanbevelingen op basis van de onderzoeksresultaten uit dit onderzoek volgen.

In de hoofdstukken 11 t/m 15 worden de mogelijk te verwachten bezwaren beschreven. Gezien de complexiteit is een aparte leeswijzer ingevoegd in hoofdstuk 10.1 Het lezen ervan is noodzakelijk om een compleet en goed inzicht te krijgen op de materie. Tegelijkertijd worden de kansen, die de aanbevelingen bieden, veel duidelijker

Aansluitend zijn er drie bijlagen toegevoegd.

Bestuurlijk Dossier:

Misbruik prepaid telefoons bij misdrijven

NB: Daar waar in dit bestuurlijke dossier wordt gesproken over een prepaid telefoon, wordt feitelijk bedoeld: een niet geregistreerde telefoon in combinatie met een niet geregistreerde simkaart. Met andere woorden: Het Imeinummer van de telefoon is niet bekend en is niet gekoppeld aan een persoon en het 06 nummer van de simkaart is niet op naam geregistreerd.

1. Inleiding

Dit dossier gaat over het onderzoek naar het misbruik van niet geregistreerde prepaid telefoons door criminelen. Eén van de bekende toepassingen van dit gebruik is bij de zogenaamde babbeltruc. De onderstaande casus was aanleiding om het onderzoek te starten en geeft een goed beeld van de problemen waar de politie mee wordt geconfronteerd.
De babbeltruc is al zo oud als de weg naar Rome en ondanks alle voorlichting en preventieacties, werkt de babbeltruc nog altijd. Vooral oudere mensen zijn vaak slachtoffer van deze ordinaire oplichters.

Criminelen die met babbeltrucs ouderen oplichten en beroven, beschikken over opvallend veel informatie van potentiële slachtoffers en lijken met lijsten te werken die onderling worden uitgewisseld.

Wie eenmaal slachtoffer is, loopt daardoor een groot risico opnieuw getroffen te worden, zo blijkt uit gesprekken met slachtoffers, slachtofferhulp en justitie. Ruim 30.000 ouderen, meestal alleenwonenden, zijn jaarlijks in hun eigen huis slachtoffer van de babbeltruc: 25.000 aan de deur en 7.000 via de telefoon.

1.1 Casus

De doelgroep (75 + die nog zelfstandig woont) wordt telefonisch benaderd door een persoon die zich voordoet als een monteur van het gasbedrijf. Hij vertelt een verhaal over een gaslek dat bij een aantal buren is geconstateerd en dat hij uit voorzorg ook even in dit huis wil kijken of alles nog oké is. Vervolgens geeft hij een goede raad om alle kostbaarheden zo snel mogelijk te verzamelen en deze op een centrale plek in het huis klaar te leggen, voor het geval dat .....! Vervolgens meldt de nepmonteur zich op het adres, pakt de tas met kostbaarheden en verlaat de woning.
Sommige slachtoffers zijn zelfs twee keer door dezelfde crimineel gedupeerd. In het tweede geval deed de oplichter zich voor als een onderzoeker van de politie of van de ING bank en vertelden dat zij dit geval aan het onderzoeken waren. Ze wisten ook precies wat er weg was. Daarop werd men binnengelaten en wederom raakte het slachtoffer geld en kostbaarheden kwijt.

1.2 Strafrechtelijk onderzoek

Onderzoek naar deze daders leverde geen concrete aanknopingspunten op. Uit de telefoongegevens (nummeronderzoek) werd duidelijk dat de daders in het overgrote deel van de gevallen gebruik maakten van prepaid toestellen van [redacted] En daar houdt ook het spoor op. Want ondanks het feit dat achterhaald kon worden dat het prepaid telefoons betroffen van [redacted] Het toestel blijft in elke casus slechts kort actief en wordt daarna vermoedelijk onklaar gemaakt en/of weggegooid. Bij elke babbeltruc (aangifte) werd, zo bleek, een ander toestel gebruikt. Deze werkwijze geeft aan dat de daders er rekening mee houden dat men toch via de telefoon kan worden opgespoord. De gebruikte telefoons kwamen in ieder geval niet uit de reguliere telefoonwinkels zoals, [redacted] etc.
De reden waarom bijvoorbeeld [redacted] worden gebruikt is duidelijk. [redacted]

1.3 Kassabon

De rechercheur heeft, om dit te bevestigen, zelf een 'fake' aankoop gedaan in een willekeurig [redacted] Ook een nepaankoop in een [redacted] leverde hetzelfde gegeven op. Het blijkt inderdaad te zijn zoals hierboven is vermeld.
Een filiaal medewerker vertelde dat er soms wel 30 toestellen tegelijk worden verkocht!

2. Probleemomschrijving

Tijdens dit onderzoek werd duidelijk dat het probleem veel meer omvattend is dan alleen de babbeltruc. Prepaid telefoons worden heel veel gebruikt bij het plegen van allerlei misdrijven. Denk hierbij vooral aan mensenhandel, heling, vuurwapen- en drugscriminaliteit, inbraken, babbeltruc, fraude, afpersing en afdreiging. Bij gebruik van prepaid telefoons blijft de beller anoniem. Logisch dat criminelen dit middel hebben omarmd. Er zijn voldoende politieonderzoeken waaruit blijkt dat anonimiteit aan criminaliteit gekoppeld kan worden.

Niet alleen criminelen maken gebruik van deze "anonimiteit". Jongeren die elkaar anoniem pesten, dreig-tweets sturen, valse 112 meldingen doen, opruiing plegen (project-X) etc. Tijdens ons onderzoek maakte [redacted] duidelijk dat zij ook intern last hebben van deze praktijken. Winkeldieven die in de winkel met elkaar bellen om ongezien hun slag te kunnen slaan

Er duiken ook steeds meer signalen op dat burgers het zat zijn dat criminelen juist vanwege deze anonimiteit veelal de dans ontspringen en niet veroordeeld kunnen worden. Dat mensen (criminelen) zich kunnen verschuilen achter deze legale anonimiteit lijkt daarom steeds meer een maatschappelijk onaanvaardbaar fenomeen te worden.

2.1 Anoniem bellen is geen recht

[redacted]

De meeste mensen hebben trouwens geen idee welke relatie het anoniem bellen heeft met criminaliteit, laat staan dat men zich realiseert welke kwalijke gevolgen dit met zich mee brengt. Daarom is de vraag of mensen bereid zijn de consequenties te accepteren die anoniem bellen met zich mee brengt, een reële vraag.

Er zijn voorbeelden genoeg van risicoacceptatie, zoals het willens en wetens deelnemen aan het verkeer terwijl we weten dat het elk moment fataal kan aflopen. Of denk aan het recht (in de VS) om wapens te bezitten. Ook stappen we massaal in het vliegtuig. Het risico dat het mis kan gaan wordt zonder problemen geaccepteerd.
Met andere woorden: Mensen zijn bereid een bepaald veiligheidsrisico te accepteren in ruil voor persoonlijke vrijheid. Afgezien van het feit dat de meeste mensen zich niet realiseren dat deze vrijheid een flinke economische schade met zich mee brengt en dat zij (zonder het te weten) daaraan financieel bijdragen, staat dit subjectieve beeld haaks op het maatschappelijk belang. De acceptatie van een bepaald veiligheidsrisico is voor elk persoon anders. De één accepteert veel meer dan de ander. De contradictie in dit verhaal is dat niemand de dupe wil worden van andermans genomen risico. Maar waar ligt de grens? Het lijkt een dilemma waarin mensen onderling nooit tot overeenstemming zullen komen. Ergo, de overheid zal verantwoordelijkheid moeten nemen ten aanzien van maatschappelijke veiligheid en zal, in dit geval, een beslissing moeten nemen t.a.v. het gebruik van niet geregistreerde prepaid telefoons.

Een kanttekening moet gemaakt worden over de gebruikte term "anoniem bellen". In feite wordt bedoeld dat het toestel en de simkaart niet geregistreerd zijn zodat de 'beller' niet opgespoord kan worden. Het bellen (communiceren) op zich, is en blijft altijd anoniem, tenzij de beller betrokken raakt in een strafrechtelijk onderzoek.

[redacted]

2.2 Omvang en ernst van dit fenomeen

Het probleem van de niet geregistreerde prepaid telefoons is groter dan gedacht. In 2011 werden volgens het CBS 1,2 miljoen (1.192.755) misdrijven geregistreerd. Daarvoor werden 372.305 verdachten aangehouden[1]. Uit de politiesystemen (fouilleringlijsten, historie printgegevens en Digitale Communicatie Sporen) kunnen we afleiden dat gemiddeld 85 % van alle aangehouden verdachten van misdrijf in het bezit is van een niet geregistreerde prepaid telefoon. Dit zijn alleen de aangehouden verdachten. Dan hebben we het nog niet eens over hun contacten. Ook blijkt uit deze systemen dat criminelen onderling vaak gebruik maken van het gratis Lebara netwerk. De cijfers over 2012 waren op sluitingsdatum van dit dossier nog niet bekend.

De niet geregistreerde prepaid telefoon lijkt een basisbehoefte te zijn voor het plegen van misdrijven.

[1] Bijalge 1 – CBS jaarcijfers 2010 en 2011 misdrijven

2.3 De essentie van het probleem

Het gebruik van een niet geregistreerde prepaid telefoon geeft (potentiële) daders het geruststellende gevoel dat zij strafbare feiten kunnen voorbereiden en plegen zonder achteraf opgespoord te worden. Sterker nog, de opsporing door politie wordt hiermee in ernstige mate bemoeilijkt zo niet onmogelijk gemaakt. De meer ervaren criminelen nemen al niet eens meer een telefoon mee tijdens de "klus", omdat bekend is dat zij via (telecom) mastgegevens de aandacht op zichzelf kunnen vestigen.

Ondanks dat de prepaid telefoon geen feitelijk wapen is, is het toch een krachtig instrument in de handen van criminelen, waarmee indirect toch slachtoffers worden gemaakt.

Criminelen willen de pakkans zo laag mogelijk laten zijn. Anonimiteit is daarbij één van de belangrijkste elementen. Doorgewinterde criminelen weten precies hoe de wetgeving in elkaar zit. Zij weten precies wat de politie wel en niet mag en maken daarbij dankbaar gebruik van deze prepaid telefoons. Maar zij begrijpen ook hoe belangrijk hun telefoon is m.b.t. de bewijslast. Ondanks dat gesprekken van prepaids niet kunnen worden herleid, staat er vaak wel informatie op het toestel zelf, zoals telefoonnummers, contactpersonen, foto's, filmpjes, etc. Het eerste wat een crimineel zal proberen wanneer hij op de hielen wordt gezeten door de politie, is het dumpen of vernietigen van zijn telefoon.

3. Doel van dit dossier

1. Met dit bestuurlijke dossier worden betrokken partijen ingelicht en bewust gemaakt van de ernst en omvang van dit fenomeen. De zo onschuldig lijkende verkoop van anonieme telefoons is blijkbaar een basisbehoefte voor het plegen van misdrijven.
2. [redacted]

3.1 Beoogd effect

Bij het nemen van de voorgestelde maatregelen (zie hoofdstuk 10: Adviezen), wordt criminaliteit tegengehouden en wordt voorkomen dat anonimiteit blijft bestaan. Ook biedt het betere mogelijkheden iemand achteraf (na een misdrijf) op te sporen. Registratie koppelt een persoon, net als bij een abonnement, aan een bepaald toestel / simkaart. Kwaadwillenden moeten weten dat zij zich niet langer kunnen verschuilen achter de anonimiteit zoals het nu werkt met de huidige prepaid telefoon. De drempel wordt voor (potentiële) daders aanzienlijk verhoogd, waardoor deze zijn "kansen" opnieuw zal moeten berekenen. Het te verwachten effect is dat het aantal misdrijven zal afnemen en dat politie en justitie meer zaken kunnen oplossen.

4. Aanpak prepaid bellen in het buitenland

Niet alleen in Duitsland, Italië, Zwitserland, Hongarije, Japan, Turkije, de meeste Afrikaanse landen, maar ook in Dubai en Singapore is het verboden om een prepaid telefoon aan te schaffen zonder dat men zich registreert. In Kenia is het zelfs verboden een niet geregistreerde telefoon bij je hebben. Overweging van de regeringen was puur het tegengaan van criminaliteit en het beter kunnen voorkomen/bestrijden van terroristische acties.

4.1 Prepaids in Duitsland

In Duitsland kent men net als in Nederland de abonnements- toestellen en de prepaid toestellen. Het aanschaffen van een prepaid simkaart kan in Duitsland net als in Nederland in de winkel of bestellen via het internet. In beide gevallen is éénmalige registratie verplicht. Het opwaarderen van je reeds geregistreerde simkaart is vrij. Ter illustratie is een willekeurig gekozen duitse telecomaanbieder als voorbeeld gebruikt. In dit geval een prepaid telefoonkaart van de [redacted] Bij de registratie worden niet alleen de NAW gegevens gevraagd, maar ook het emailadres en deze gegevens worden gekoppeld aan het bankrekeningnummer van de aanvrager.Voor meer informatie zie [redacted]

Een voorbeeld van het "registrierungsformular" voor prepaidsimkaarten is bijgevoegd in bijlage 4.

De registratie wordt geregeld in §111 TKG (Telekommunikationsgesetz) van de Duitse telecommunicatiewet. Hierin staat dat een Telecomaanbieder pas een simkaart mag vrijgeven nadat de aanvrager zich heeft geregistreerd. Er wordt daarbij geen onderscheid gemaakt tussen een abonnenment of prepaid.
Echter in de praktijk blijkt dat de controle op de juistheid van de gegevens niet uniform is geregeld. Bij enkele Duitse telecomaanbiedersaan [redacted] is het mogelijk om onjuiste (valse) gegevens in te vullen. De Duitse politie geeft aan dat ondanks de vele fraude gevallen er wel veel meer zaken opgelost worden en dat dit een behoorlijke capaciteitswinst met zich meebrengt. Zie verder hoofstuk 11.2 en verder)

4.2 Prepaids in Kenia

Dat dit probleem (misbruik van niet-geregistreerde prepaid telefoons) ook in andere landen speelt mag blijken uit onderstaande berichten:

Spits. wo 02 jan 2013, 16:21

'Anoniem' bellen? Drie jaar cel

In Kenia is het vanaf vandaag verboden om registratieloos mobiel te bellen. De Keniaanse minister van Communicatie Bitange Ndemo heeft laten weten wie de nieuwe wet overtreedt, drie jaar de cel in kan verdwijnen.

De regering van het Oost-Afrikaanse land hoopt met de maatregel misdaad en terrorisme beter te kunnen indammen. Ook hoopt de regering te voorkomen dat "haatboodschappen" worden verspreid in de aanloop naar de presidentsverkiezingen in maart.

Rond de vorige gang naar de stembus in 2007 vielen door politiek geweld meer dan 1000 doden.

Het Keniaans reglement van de grootste telecomaanbieder CCK vind je hier:
http://www.cck.go.ke/sim_registration/index.html

Ook in Rwanda, Zambia, Tanzania, Nigeria en Oeganda geldt het verbod op ongeregistreerd bellen al enkele jaren. The Independent schrijft hierover:" The registration is intended to help law enforcement agencies identify SIM card owners, track criminals using phones, curb loss of phones through theft, nuisance/hate speech, fraud, threats and inciting violence.
http://www.independent.co.ug/news/news/7164-ucc-will-not-extend-sim-card-registration-period

Het Oegandees reglement van de grootste telecomaanbieder MTN lees je hier:
http://www.mtn.co.ug/MTN-Sim-registration.aspx

4.3 Terroristen zijn oorzaak van het verbod op anoniem bellen

Criminelen en terroristen gebruiken graag prepaid telefoons, aangezien men hier anoniem mee kan bellen. Men hoeft zich immers niet te legitimeren bij de aankoop van een prepaid toestel. Dat is nu afgelopen, in Zwitserland althans.

De Zwitserse overheid nam dit besluit al in 2003 omdat Al Qaeda terroristen in het verleden gebruik hebben gemaakt van Zwitserse prepaid toestellen. Onder deze terroristen zaten ook de kapers van de vliegtuigen die zich in het World Trade Center boorden, op 11 september 2001.

Vandaar dat vanaf 2003 iedereen die een prepaid telefoon of SIM-kaart koopt zich moet legitimeren. De mobiele operators moeten deze gegevens minimaal twee jaar lang bewaren.

In Somalië overweegt men deze maatregel in het kader van criminaliteit, maar met name om de piraterij op zee en de daarbij behorende ontvoeringen, het hoofd te kunnen bieden.

[redacted]

Ter illustratie – op de website van de Turkse telecomaanbieder [redacted] wordt vermeld:

"According to regulations in Turkey, the operator is required to know the identity of prepaid SIM card holders. These regulations apply for all Turkish SIM Cards, both for citizens of Turkey as well as foreigners".

The operator requires that a **photo copy of your passport** is attached in order for them to activate your SIM card. An image upload URL is attached in your order confirmation e-mail.

4.4 Dreigingniveau terrorisme verhoogd

De link naar terrorisme komt niet helemaal uit de lucht vallen. Zoals gezegd hebben vele landen waaronder Zwitserland ter bestrijding hiervan het anoniem bellen verboden. Mocht de perceptie bestaan dat al die ernstige feiten en terroristische acties alleen maar in het buitenland gebeuren, kan het onderstaande bericht u wellicht een beter beeld geven van de realiteit.

Foto: René Oudshoorn

DEN HAAG - (Telegraaf 13 mrt 2013, 10:33)
Het is voorstelbaar dat Nederlandse jihadstrijders die terugkeren uit Syrië een aanslag willen plegen in Nederland. Hoewel er geen concrete aanwijzingen zijn voor een aanslag, heeft de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) Dick Schoof woensdag het dreigingsniveau voor terrorisme verhoogd naar het een na hoogste niveau.

Het is voor het eerst sinds 2009 dat het niveau 'substantieel' (niveau 3 van 4) van kracht is. Sinds november van dat jaar gold het niveau beperkt (niveau 2 van 4). De burgers op straat merken niets van de verhoging en ze hoeven zich geen zorgen te maken. Schoof zegt dat onder meer de geheime dienst AIVD en de politie „hun alertheid hebben verhoogd en hun inspanningen hebben geïntensiveerd".

Het verhoogde dreigingsbeeld staat volgens Schoof volledig los van de troonswisseling op 30 april. Dat de NCTV heeft besloten het niveau aan te passen, heeft vooral te maken met de mogelijke dreiging die uitgaat van teruggekeerde jihadreizigers.

Een kleine 100 strijders uit Nederland zijn afgereisd naar oorlogsgebieden, voornamelijk Syrië, maar ook naar diverse landen in Afrika. Volgens de NCTV kunnen de jihadstrijders bij terugkomst door hun strijdervaring een veiligheidsrisico opleveren. Ze zijn bij terugkomst niet alleen radicaal in hun gedachtegoed, maar kunnen ook getraumatiseerd zijn en mogelijk bereid zijn om geweld te gebruiken.

Deze jihadgangers kunnen ook een risico vormen voor Westerse doelen in de gebieden waar zij naar toe reizen en „bestaat de mogelijkheid dat zij andere geestverwanten uit Nederland aansporen hen te volgen",

waarschuwt Schoof. Hij noemt het medeleven en het hulp bieden aan de Syrische burgers „begrijpelijk". „Onze zorg zit op degene die gaan strijden."

Hij zegt dat in Nederland signalen zijn die erop duiden dat jihadistische radicallsering van kleine groepen jongeren in ons land is toegenomen. „Ook blijkt dat de doorradicalisering naar geweldsbereidheid soms zeer snel kan verlopen." Schoof constateert tegelijkertijd dat de aandacht van de politiek en in de samenleving voor radicalisering de laatste jaren juist is afgenomen.

De autoriteiten proberen te voorkomen dat jongeren naar jihadistische trainingskampen of strijdgebieden afreizen en houden teruggekeerde strijders in de gaten. „Het gaat daarbij onder meer om inlichtingen en onderzoek, opsporing en vervolging." Zo verhoogt de marechaussee de controles aan de grenzen. In een brief aan de Tweede Kamer schrijft minister Ivo Opstelten dat ook de burgemeesters van de 4 grote steden al op de hoogte zijn gebracht van de ontwikkelingen.

In Europa gaat het om vele honderden strijders. Andere Westerse landen hebben daarom ook hun zorgen geuit en hebben maatregelen genomen.

[redacted]

4.5 Opsporing

De prepaid telefoons worden niet alleen gebruikt om anoniem te kunnen communiceren onderling, maar ook voor communicatie met potentiële slachtoffers van oplichting / babbeltruc. Sommige criminelen gebruiken zelfs voor elke gesprek een ander (nieuw) toestel en/of simkaart. Dat maakt het onmogelijk telefoongesprekken en misdrijven aan elkaar te linken, laat staan personen eraan te koppelen. Prepaid telefoons zijn wel via het telefoonnetwerk te traceren, maar het is niet mogelijk om de eigenaar of de beller te achterhalen. Het unieke Imeinummer van zo'n telefoon, wordt bij de aankoop niet op naam gesteld /geregistreerd en/of wordt niet aangemeld bij een netwerkprovider.

[redacted]

5. Verkoop van prepaid telefoons

Er zijn vier soorten winkels die prepaid telefoons verkopen.

1. **Telefoonwinkels** [redacted]
2. **Supermarktketens** [redacted]
3. **Webwinkels (online)**
4. **Uit recycling bij belwinkels** (illegale circuit)

Onder 1. Bij de telefoonwinkels (vakhandel) wordt het Imeinummer en het serienummer van prepaid telefoons standaard op de kassabon geregistreerd. Dat is overigens niet gegarandeerd. Zij doen dit uit eigen belang, omdat het verkopen van telefoons hun specialiteit, hun core-business is. Het is hun bestaansrecht en kunnen zich daarom geen negatieve reclame permitteren. Registratie is belangrijk bij de serviceverlening en het tegengaan van garantiefraude. Daarnaast voorkomt het interne winkeldiefstal. Alleen bij speciale aanbiedingen, waarbij meerdere producten in één pakket worden aangeboden is het mogelijk dat het Imeinummer niet meer vermeld wordt, maar dat bv het simkaartnummer leidend is.

Onder 2. Bij de supermarkten en warenhuizen is dit een heel ander verhaal. Daar wordt helemaal niet geregistreerd. Reden om niet te registreren is puur economisch. Deze winkels verkopen prepaid telefoons zonder enige vorm van registratie. Op de kassabon wordt alleen het artikelnummer geprint en dat nummer is voor alle telefoons in die winkel hetzelfde. Geen contract, geen registratie en geen kredietcheck.

Onder 3. Bij het online kopen van een prepaid telefoon is het niet altijd zeker dat het Imeinummer op de factuur wordt vermeld. Ook hier is het registreren afhankelijk van het soort webwinkel. In principe worden op de factuur de naam en adresgegevens van de koper en het Imeinummer van het toestel vermeld. Maar in sommige gevallen heeft de tussenhandel (bv [redacted] een pakketaanbieding van een toestel icm een simkaart. Dat wordt verpakt in een mooi doosje van de tussenhandel en vanaf dat moment is het simnummer leidend. Normaal gesproken zijn door de aankoop de bank- en adresgegevens van de koper bekend, maar het is ook mogelijk zendingen onder rembours te laten bezorgen op een ander- dan het huisadres.

Onder 4.
Oude mobiele telefoons kunnen worden ingeleverd voor geld. De mobiele telefoons worden zorgvuldig nagekeken. De toestellen die nog goed werken worden doorverkocht in verschillende landen over de gehele wereld. Mobiele telefoons die niet meer werken worden zorgvuldig gerecycled. De grondstoffen worden weer opnieuw gebruikt.

Er zijn twee mogelijkheden om je oude mobiel te verkopen, via internet en in de winkel. Bij de [redacted] kun je je oude mobiele telefoon inleveren tegen een bepaald bedrag. Het oude toestel wordt bekeken en de restwaarde wordt bepaald. Dat wordt bij de kassa uitbetaald.
Bij de bekende telefoonwinkels [redacted] kunnen oude telefoons worden ingeruild op een nieuwe. In principe betalen de 'vakwinkels' niet contact uit bij het innemen van een gebruikte telefoon. Bij inlevering van oude telefoons wordt het bedrag per bank overgemaakt.

[redacted]

5.1 Aantallen prepaid telefoons

Volgens de marktcijfers van de OPTA waren er aan het einde van 2011 21,8 miljoen mobiele aansluitingen, waarvan 10,6 miljoen abonnementen en **6,2 miljoen prepaid**[2]. Het aantal abonnementen met mobiel breedband is in een jaar tijd met een miljoen toegenomen tot 8,7 miljoen. Daaronder vallen 7,6 miljoen smartphones en 1,1 miljoen mobiele internetabonnementen voor onder andere tablets en laptops. Circa 1 miljoen aansluitingen worden gebruikt voor machine-to-machine toepassingen.

[2] Bijalge 3 – OPTA tabel aantallen en omzet

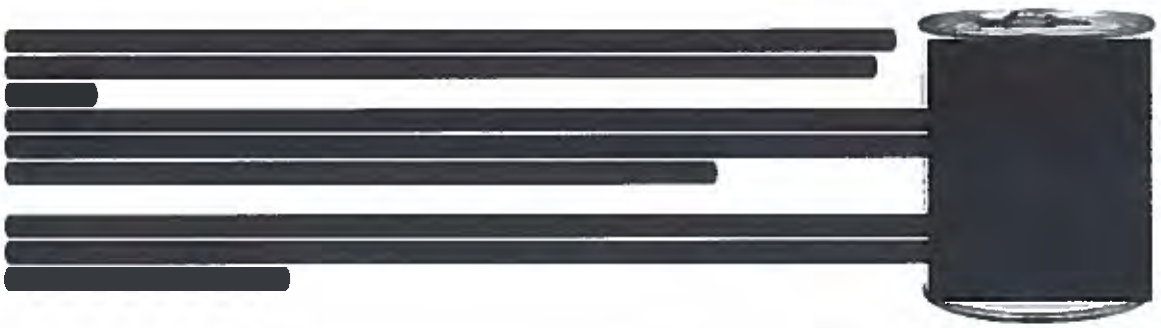
6. Maatschappelijke relevantie

[redacted]Het hebben van een niet geregistreerde prepaid telefoon maakt dat criminelen een drempel over durven gaan, die anders te hoog zou zijn. Het ligt in de lijn der verwachting dat het gebruik van prepaid telefoons alleen maar zal toenemen.[redacted]

[redacted]

[redacted]t

(advertentie) Voordelig prepaid bellen begint[redacted]



[redacted] Eens in de zoveel tijd wordt het assortiment ververst en iedere twee of drie weken is er een extra scherpe aanbieding.

6.1 Wederzijdse belangen

[redacted]

Het zou naïef zijn van ondernemers om te denken dat het hen zelf niet zou kunnen raken. De branche wordt immers zelf ook duizenden malen per jaar slachtoffer van overval, diefstal of bedrijfsinbraak, waarbij hoogst waarschijnlijk gebruik werd gemaakt van een prepaid telefoon.

6.2 Handhaving

[redacted] De combinatie tussen handhaven en stimuleren/voorlichten is namelijk groter dan de som der delen. 'Handhaving' is geholpen met voorlichting: ondernemers weten beter waarom ze iets moeten doen, hoe ze het moeten aanpakken en wat de voordelen zijn. 'Voorlichting' over maatregelen heeft veel effect als de ondernemers weten dat ze er daadwerkelijk wat mee moeten doen en erop gecontroleerd worden.
Het staat de ondernemer vrij te kiezen hoe hij vorm wil geven aan deze adviezen. Uit gesprekken met groot winkelbedrijven blijkt dat het implementeren van het serienummer op de kassabon een kostbare zaak is. Aan de andere kant, biedt registratie ook weer voordeel t.a.v. garantiefraude.

6.3 [redacted]

[redacted]

7. Onderzoek Apollo 2008

Het misbruik van prepaid telefoons werd al in 2008 gesignaleerd. In het rechercheonderzoek "Apollo" van de BR's Haarlem, Den-Haag, Amsterdam en Rotterdam werd dit probleem al onderkend en naar aanleiding van het onderzoek werd geadviseerd de identificatie- en registratieplicht uit te breiden. Het NRC van 9 mei 2008, schreef hierover het volgende:

http://www.nrc.
"Rotterdam, 9 mei 2008. Prepaidtelefoonkaarten mogen niet meer anoniem worden aangeschaft. Bezoekers van internetcafés, belhuizen en bibliotheken zouden zich moeten identificeren om computers te mogen gebruiken.

Deze uitbreiding van de identificatie- en registratieplicht bepleiten de vier Bovenregionale rechercheteams van Haarlem, Den Haag Amsterdam en Rotterdam. Deze teams deden de afgelopen jaren het zogeheten Apollo-onderzoek naar met name het wegsluizen van illegaal verdiend geld door Nigeriaanse criminele bendes. De praktijken staan in het tot dusverre niet openbaar gemaakte rapport Misbruik van Money Transfers, dat de resultaten van het Apollo-onderzoek beschrijft.

Uit het Apollo-onderzoek onder leiding van het bovenregionale rechercheteam Noordwest en Midden-Nederland vloeit ook de aanbeveling voort de controle op echtheid van identiteitsbewijzen te verbeteren, met name in geldtransactiekantoren die internationale overboekingen (money transfers) uitvoeren. Uit het Apollo-onderzoek bleek dat West-Afrikaanse en andere buitenlandse criminelen op grote schaal gebruikmaken van money-transferkantoren. Ook maken ze gebruik van de mogelijkheid om zonder persoonsregistratie te bellen en anoniem e-mailberichten te versturen.

Medewerkers van transactiekantoren controleren de identiteitspapieren van klanten onvoldoende, hetzij uit angst voor represailles van geweigerde klanten, hetzij uit onbekendheid met buitenlandse identiteitspapieren of uit laksheid. Daardoor maken internationaal opererende criminelen in toenemende mate gebruik van deze vorm van internationale geldoverdracht.

Gebruikten criminelen tot voor kort vooral bankrekeningen op naam van 'katvangers' om geld te ontvangen, nu gebeurt dat via kantoren van Western Union, MoneyGram en andere geldtransactiekantoren. De identiteitscontrole is daar „verre van optimaal". Criminelen doen soms verscheidene keren per dag, meermalen per week transacties met valse papieren. De onderzoekers willen dat money-transferkantoren 'klantenprofielen' opstellen. Ook zou het aantal kantoren in een bepaald gebied beperkt moeten worden. Voorts suggereren zij een geldtransactie die via een money transfer loopt te koppelen aan een bankrekening.

Uit het politieonderzoek is verder gebleken dat de opsporing werd belemmerd door de afwezigheid van een registratieplicht voor bezoekers van internetcafés, belhuizen of bibliotheken en doordat er geen registratieplicht geldt voor het gebruik van prepaid telefoonkaarten. De politie bepleit daarom ook aanbieders van openbare communicatiediensten onder de Wet Bevordering Integriteits beoordelingen door het Openbaar Bestuur (Bibob) te brengen.

7.1 Advies uit onderzoek Apollo

Uiteindelijk is met het advies uit dit onderzoek niets gedaan. Daar liggen een aantal oorzaken aan ten grondslag.

Zoals in het "Apollo" onderzoek wordt aangegeven dat aanbieders van openbare communicatiediensten (belwinkels) onder Wet Bibob zouden moeten vallen is een maatregel die gericht is op een individuele telecomaanbieder en niet op de totale branche. Het lijkt net een stap te ver en zal o.i. op zich niet leiden tot het voorkomen van misdrijven waarbij de daders prepaid telefoons gebruiken. De "Bibob" maatregel is wel een "stok achter de deur maatregel" en is veel meer opsporingsgericht (nadat het feit is gepleegd). De focus in dit dossier is juist gericht op het verstoren van het daderproces, met als beoogd effect dat de dader afziet van zijn voornemen om een strafbaar feit te plegen (Tegenhouden)

8. Prepaid discussie is niet nieuw

De gedachte om ongeregistreerd bellen te verbieden is niet nieuw. De hele "prepaid" discussie is in 1998 al gevoerd. [redacted]

Anno 2013 liggen de zaken heel anders. Het aantal prepaid gebruikers is enorm toegenomen. [redacted] Daarnaast zijn de technieken en methodieken sterk verbeterd waardoor we in staat zijn om de zogenaamde katvangers tegen te gaan.

8.1 Reactie van College Bescherming Persoonsgegevens

Naar aanleiding van bovenstaand artikel van het Apollo onderzoek (9 mei 2008) reageerde de NOS dat het CBP niets in de voorstellen ziet. Volgens het College zou Nederland zich op een 'glijdende schaal' gaan begeven als de voorgestelde maatregelen door de regering worden overgenomen, omdat alle Nederlanders een groot deel van hun privacy zouden moeten inleveren. Ook private speurders zien weinig heil in de maatregelen; de netwerken zouden zich razendsnel aanpassen aan een nieuwe situatie, bijvoorbeeld door mobieltjes uit het buitenland te betrekken en zelf clandestiene internetcafé's te openen. http://life.tweakers.net/nieuws/53391/justitie-wil-vergaande-maatregelen-aanpak-internetfraudeurs.html

8.2 Relatie tussen ontwikkeling technologie en criminaliteit

Het standpunt van het CBP dateert uit 2008. Inmiddels zijn we vijf jaar verder en hebben zich wereldwijd nogal wat veranderingen aangediend. Denk hierbij alleen al aan het aantal mobiele telefoons dat momenteel in omloop is. Alleen in Nederland spreken we in 2012 over 21,7 miljoen mobiele telefoons, waarvan 6,2 miljoen prepaids (cijfers Opta).
Denk ook aan de opkomst van de camera in de mobiele telefoon, de mogelijkheid om foto's van hoge kwaliteit te versturen. Ook de breedbandverbinding (internet) deed zijn intrede. Filmpjes kijken, opnemen en versturen. Het toenemende gebruik van internet applicaties (apps) zoals Navigatie, WhatsApp, Pingen, Google, GPS, etc.
De vooruitgang en ontwikkeling van de technische mogelijkheden is ongekend maar heeft als neveneffect dat bepaalde personen deze technologie ook gebruiken en inzetten bij het plegen van criminaliteit. De verwachting is dat dit de komende jaren nog verder toeneemt.

De vraag komt dan ook niet als een verassing. Accepteren we dit neveneffect als onvermijdelijk gevolg van onze welvaart of zijn de grenzen bereikt en nemen we maatregelen om (zware) criminaliteit tegen te houden?

Toegegeven, de opsporing heeft ook baat gehad bij die technische ontwikkelingen, [redacted] Er gebeuren meer misdaden dan we aankunnen (onderzoeken). De opsporing heeft ernstig last van de anonimiteit en de tijd die dergelijke onderzoeken kosten. [redacted] Zie voor verdere uitleg het hoofdstuk Uitwerking Advies op pagina 24 ev.

[redacted]

8.3 Vrijheid van meningsuiting

Komt de vrijheid van meningsuiting dan in het gedrang wanneer er een verplichting komt om prepaid telefoons te registreren, of anders gezegd een verbod op anonimiteit?

De bezwaren die bestaan tegen het verbod op "anonimiteit" zijn gebaseerd op de angst dat men niet meer zeker kan zijn van bescherming van het communicatiegeheim. (art 8 EVRM).
In 2006 werd het proefschrift gepubliceerd "Anoniem Communiceren: van drukpers tot weblog", van Dr. Anton Dekker, waarin hij de "grondrechtelijke bescherming van anoniem communiceren" uitlegt.
Hij stelt dat de anonieme verspreiding van informatie door de tijden heen maatschappelijke betekenis heeft gehad en er is een direct historisch verband tussen verboden op anonimiteit en de uitoefening van censuur. Anonimiteit maakt censuur immers onmogelijk. Streng voorafgaand toezicht op de inhoud van geschriften dient dus te worden ondersteund door verboden op anonimiteit. Alleen dan kunnen ongewenste politieke en religieuze uitingen effectief worden bestraft en bestreden.

De maatregelen tegen anonimiteit richtten zich in de eerste plaats tegen tussenpersonen zoals de drukker, de uitgever, de boekverkoper en de journalist. Zij waren immers degenen die de geschriften verveelvoudigden en verspreidden. Reeds vroeg was het gezag erop bedacht een middel uit te denken om tot de oorsprong van de misdadige gedachte te kunnen opklimmen teneinde de verdere verspreiding van gevaarlijke ideeën te beletten. Door drukkers en uitgevers streng te straffen maar hen straffeloosheid of strafvermindering in het vooruitzicht te stellen wanneer zij de schrijver bekend maakten, werd getracht om de verantwoordelijke op te sporen.
Dr. Dekker besluit zijn conclusie met:
Ook de wetgever lijkt uit de geschiedenis een belangrijke conclusie te hebben getrokken: als het verbod op anonimiteit een middel is om de inhoud van informatie preventief te controleren en te sanctioneren, dan volgt daaruit dat werkelijke uitingsvrijheid niet kan bestaan wanneer men te allen tijde verplicht is om op een geschrift zijn naam te vermelden. (Zie proefschrift Dr. A. Dekker op http://dare.uva.nl/document/19656)
De conclusie van Dr. Dekker is duidelijk, zonder de mogelijkheid anoniem te communiceren, kan vrijheid van meningsuiting niet bestaan.

8.4 Verkeerde voorstelling van zaken

[redacted] zullen al gauw verwijzen naar dit onderzoek. Echter het onderzoek van Dr. Dekker gaat over het anoniem "schriftelijk" kunnen communiceren.

Dit geeft het begrip "communiceren" in onze context een andere betekenis. In ons dossier gaat het over "mondelinge communicatie". Gesprekken tussen personen met behulp van een telefoon. Hierdoor vervallen de bezwaren van de drukkers, de uitgevers en providers. [redacted] Het CBP maakt zich bijvoorbeeld bij de providers wel zorgen over de opslag van de registraties (persoonsgegevens), maar dat is in dit dossier niet aan de orde.

Ondanks het feit dat een telefoon geregistreerd is, blijft het anonieme gesprek op zichzelf gewoon bestaan. [redacted] Pas op het moment dat één en ander in verband kan worden gebracht met een misdrijf, wordt het voor politie en justitie mogelijk de tenaamgestelde van het toestel te achterhalen. Daarmee is niet achterhaald wat het gesprek is geweest. Wat dat betreft veranderd er niets. De verandering (verbetering) zit in de mogelijkheid iemand achteraf snel te kunnen achterhalen. [redacted]

9. Conclusies

- Het plegen van criminaliteit met het op legale wijze verkregen hulpmiddel (niet geregistreerde prepaid telefoon)zoals omschreven in dit dossier, is een mooi voorbeeld van hoe de onderwereld en de bovenwereld met elkaar verweven kunnen zijn.
- Het fenomeen is volledig geaccepteerd in de maatschappij en [redacted]
- [redacted]
- [redacted] mmers de bedoeling van een prepaid telefoon is niet om anoniem te kunnen bellen en om criminaliteit te kunnen plegen, maar juist om mensen die heel weinig bellen een alternatief te bieden ten opzichte van een (te)duur telefoonabonnement.
- [redacted] Ook de Telecomproviders spelen een rol als het gaat om het tot stand brengen van een telefoon verbinding terwijl niet bekend is wie de verbinding inhuurt.
- Uit het dossier wordt voldoende duidelijk dat criminelen gebruik maken van legale maatschappelijke processen en structuren. Het beschreven probleem is allang geen incident meer. [redacted]
- Een andere constatering is dat de verkoop van prepaids ook bij de reguliere vakhandel absoluut geen garantie is dat altijd het Imeinummer wordt vermeld op de kassabon.
- [redacted]

10. Adviezen

Alle betrokken partijen dienen hun systemen en procedures op de genoemde adviezen aan te passen en actief te participeren.

10.1 Waarom zijn hoofdstuk 11 – 15 nog nodig

Het is te verwachten dat er vanuit diverse kanten bezwaren zullen zijn tegen dit advies. Daarom is het noodzakelijk dat de verwachtte tegenargumenten nader worden benoemd en toegelicht.

Bedreigingen en registratie ervaringen in het buitenland (hfst 11)

Moeten de goeden onder de kwaden lijden? (hfst 12)

Het aanmelden met valse naam (hfst 12)

Katvangers (hfst 12)

Privacy aspecten (hfst 13)

Het Burgerservicenummer en het "kopietje paspoort" (hfst 13)

Het gebruik van buitenlandse simkaarten (hfst 14)

Kostenplaatje (hfst 15)

11. Bedreigingen en bij-effecten van registratie

Om iedere prepaid bezitter te overtuigen dat hij/zij het toestel en de simkaart moet registreren is heel eenvoudig. Ieder telefoonnummer waaraan geen naam is gekoppeld (niet geregistreerd) krijgt standaard geen verbinding (ook niet vanuit Nederland naar het buitenland). Daarvoor is het nodig dat wettelijk geregeld wordt dat niet geregistreerd bellen strafbaar wordt. Op basis daarvan kunnen providers de doorgifte (verbinding) van deze anonieme gesprekken weigeren. Eerst registreren en betalen.

[redacted] Gestolen of vermiste mobiele telefoons kunnen niet zomaar meer worden voorzien van een 'nieuwe' prepaid kaart. Want bij aanmelding zal blijken dat de telefoon gestolen is of vermist. Het gevolg is dat de registratie niet doorgaat en dat de aanvrager wordt doorgemeld aan de politie. Is bij het aanmelden nog niet bekend dat het toestel is gestolen dan wordt later, op basis van de werking van de verplichte IMEI-Blokking, dat medio 2014 operationeel wordt, het Imeinummer van dat toestel wordt geblokkeerd zodat bellen niet meer mogelijk is.

Dit positieve bij-effect ontstaat natuurlijk alleen indien bij wet geregeld wordt dat niet geregistreerd bellen strafbaar is.

11.1 Bellen met een buitenlands simkaartje

Veel criminaliteit is grensoverschrijdend. Dat geldt ook voor het telefoonverkeer.[redacted] Op dit moment is het bijvoorbeeld mogelijk om met in het buitenland anoniem gekochte prepaid simkaarten ook gewoon in Nederland te bellen.[redacted]

Het kan nog extremer; uit onderzoeken weten we dat criminelen met een simkaart uit bv een ander werelddeel (Afrika, Rusland) via het netwerk uit dat land (werelddeel) in Nederland kunnen bellen. Men maakt hierbij gebruik van de zogenaamde "roaming services" van de providers. Dat kost heel veel geld, maar dat maakt die criminelen blijkbaar niet uit. Men wil koste wat kost anoniem blijven.[redacted] Zoals eerder genoemd hebben landen als Duitsland en Italië al een dergelijke regeling.

Met het uitvoeren van bovenstaande adviezen zijn natuurlijk de problemen rondom de anonimiteit niet in één keer opgelost. Het internet biedt naast de telefonie nog talloze mogelijkheden om anoniem te communiceren. [redacted]

11.2 Registratie in het buitenland

[redacted] Dit onderwerp werd vervolgens ter sprake gebracht tijdens de Internationale Conferentie (Interceptie) in juni 2013. In meerdere Europese landen worden momenteel prepaids geregistreerd. In het algemeen is men er goed over te spreken. Maar er zijn natuurlijk ook andere geluiden. Vooral in Italië en Duitsland wordt veel gefraudeerd bij de registratie. Er wordt veel gebruik gemaakt van katvangers. Exacte cijfers zijn niet bekend. Dit zou een argument kunnen zijn om van verdere actie af te zien. [redacted] Kennelijk is de behoefte aan 'anonieme' prepaid telefoons bij criminelen erg groot. Zo groot zelfs dat er op grote schaal wordt gefraudeerd bij de registratie. [redacted] Nu we weten hoe de fraude wordt gepleegd is het vrij simpel om maatregelen te bedenken die dit kunnen voorkomen (zie 12.2) De Duitse politie geeft trouwens wel aan dat ondanks de vele fraude gevallen er wel veel meer zaken opgelost worden en dat dit een behoorlijke capaciteitswinst met zich meebrengt. Ook Ierland liet weten bezig te zijn registratie bij prepaids in te voeren.

12. Goedwillenden vs kwaadwillenden

Het feit dat anonieme prepaid telefoons veel voorkomen bij criminelen en andere kwaadwillenden, betekent overigens niet dat alle personen met anonieme prepaid telefoons kwaad in de zin hebben. Ook journalisten gebruiken deze vorm van anonieme communicatie voor bronbescherming. Zeker nu via mobiele telefonie – en zeker smartphones in combinatie met vele apps - heel veel zaken bij vele (niet overheids-) partijen bekend zijn (plaatsen, tijden, inhoud communicatie, contacten et cetera) hebben sommigen behoefte aan anonimiteit. Met registratie wordt, zo wordt gedacht, voor 'goedwillenden' ook de mogelijkheid tot anonimiteit ontnomen.
Zoals al eerder in dit dossier is aangehaald, is de waarborg en zekerheid van anonimiteit geheel afhankelijk van de gebruiker zelf. Bij de registratie wordt niet naar het beroep gevraagd. Ondanks dat iedere gebruiker geregistreerd staat wordt dit niet door de overheid gemonitord. Pas na gebleken betrokkenheid bij misdrijven, kan deze anonimiteit doorbroken worden.

12.1 Verschil tussen "anoniem bellen" en "Niet geregistreerd bellen"

Om verwarring te voorkomen moet duidelijk worden dat anoniem bellen niet hetzelfde is als ongeregistreerd bellen. Veel mensen denken dat met het registreren van de telefoon je niet meer anoniem kunt bellen, dat iedereen kan zien met wie je belt en dat de gesprekken kunnen worden afgeluisterd. Dat is pertinent niet juist. De gesprekken die mensen met elkaar voeren zijn en blijven volledig anoniem, tenzij zij als verdachte worden aangemerkt in een strafrechtelijk onderzoek. Dan kan justitie in bepaalde gevallen toestemming verlenen om gesprekken van die verdachten af te luisteren. Dat laatste maakt overigens geen verschil met de huidige gang van zaken, want op dit moment werkt het namelijk net zo.

[redacted]

Anoniem communiceren blijft altijd mogelijk. Je weet immers niet wie de telefoon feitelijk gebruikt. Alleen het bezit en de simkaart van de telefoon worden geregistreerd; niet de gebruiker en ook niet inhoud van de gesprekken. Ook een vast internetadres is eigenlijk anoniem. Want een persoon identificeren aan de hand van het IP adres kan niet. Je kunt het adres wel opsporen, maar dan is nog niet bekend wie er achter de computer heeft gezeten. Je kunt ook makkelijk internetten in een internetcafé of een proxy gebruiken. Daarnaast zijn er diensten zoals 'Skype' of de zogenaamde TOR-netwerken die anoniem communiceren mogelijk maken. Een 'fake' email adres is ook zo aangemaakt. Er zijn zelfs websites die een tijdelijk nep emailadres aanbieden. Vervolgens komen de 'katvangers' weer in beeld, of nog erger je wordt beroofd van je werkende telefoon. Dit laatste delict wordt trouwens in 2014 aangepakt met de invoering van het zogenaamde 'IMEI-Blokking'. Een verplichte registratie voor alleen mobiele telefoon en simkaarten zou kunnen leiden tot slechts een verschuiving van het probleem. Men zal gaan zoeken naar andere methoden: buitenlandse simkaarten, fraude bij registratie of fraude met persoonsgegevens. [redacted]

12.2 Aanmelden /registreren met valse naam

Kwaadwillenden zullen proberen zich te registreren onder een valse naam. Dat is via het internet niet moeilijk. Je vult gewoon een andere naam, andere geboortedatum en een ander adres in. Het wordt pas moeilijk als je wilt betalen onder diezelfde valse naam. De tenaamstelling van de bankrekening klopt dan niet met de opgegeven naam. Daarmee geef je aan dat er eigenlijk iemand anders jou rekening gaat betalen. Je zou dan alsnog anonimiteit in de hand werken. In de website van de provider zou die mogelijkheid verhinderd moeten kunnen worden.
De volgende voorwaarden kunnen gesteld worden:

1. Betaling wordt alleen geaccepteerd als de naam van de tenaamgestelde van de bankrekening overeenkomt met de naam van de aanvrager.
2. De op naam geregistreerde simkaart werkt alleen op het toestel waarvoor de aanvraag is gedaan. (simkaart wordt gekoppeld aan het Imeinummer)

Bij het kopen van een prepaid in de winkel zou het bij het registreren wel mis kunnen gaan. Bijvoorbeeld: de koper geeft een valse naam op en identificeert zich met een gestolen identiteitskaart / paspoort. Ondanks dat er fotokopie wordt gemaakt van de ID kaart (wat overigens verboden is bij Wet) kan er daarna ook nog met een gestolen pinpas worden betaald. Om dit tegen te gaan moet een solide systeem / protocol worden bedacht, zonder dat het personeel het idee krijgt een verlengstuk te worden van de politie. Bijvoorbeeld dat bij de verkoop van een "prepaid" dezelfde procedure gevolgd wordt als bij een "abonnement" (Check/dubbel check). Daarnaast kan worden nagedacht om een dergelijke procedure in het systeem te bouwen zodat "het personeel" hierin geen fouten meer kan maken.
Ten overvloede wordt opgemerkt dat het aanmelden / registreren onder een valse naam strafbaar is gesteld in artikel 225 van het Wetboek van Strafrecht (valsheid in geschrifte). Natuurlijk zijn er op dit onderwerp de nodige varianten en uitzonderingen te bedenken. Het gaat te ver om deze in dit dossier allemaal te behandelen. Deze zullen in overleg met de betrokken partners moeten worden uitgewerkt.

12.3 Katvangers

Katvangers zijn een serieuze bedreiging in dit geheel. De ervaring leert dat na genomen maatregelen er altijd een nieuwe beweging, een nieuwe criminele modus ontstaat. Criminelen vinden altijd weer een nieuwe manier om (in dit geval) anoniem te blijven. Bij invoering van verplichte registratie zullen criminelen meer gebruik gaan maken van de zogenaamde 'katvanger', Hoe werkt dat precies?

Bij invoering van de voorgestelde maatregelen tot registreren is het bij de huidige wetgeving niet verboden dat iemand bv 1000 prepaid telefoons koopt, deze allemaal op zijn eigen naam geregistreerd en vervolgens doorverkoopt aan anderen. Op deze manier wordt de regelgeving handig omzeild. Ook vervalt daarmee het beoogde effect. Er zullen daardoor nieuwe- en andere spelers in beeld komen. Namelijk handelaren die een centje willen bijverdienen en op deze manier "anonieme" telefoons te koop aanbieden. Het misbruik van junks of anderszins jongeren die onder bedreiging moeten fungeren als katvanger zal daardoor naar verwachting afnemen. De eerst genoemde variant is veel waarschijnlijker en veel eenvoudiger.

Hoe lossen we dit op? Kunnen we de registratiestructuur van prepaid telefoons zo inrichten dat het fenomeen katvangers onmogelijk wordt of in ieder geval zinloos wordt? Uiteraard is bij het bedenken van een dergelijke tegenmaatregelen de kennis en ervaring van de commerciële partners nodig, maar één van de mogelijkheden is het stellen van eisen/voorwaarden t.a.v. het aantal toestellen / simkaarten dat één persoon maximaal op naam mag stellen / hebben. [redacted]
Wordt het systeem daarbij ook nog eens aangesloten op de database van stopHeling.nl dan komen op deze manier alle gestolen telefoons ook snel boven water.

[redacted] Daarnaast biedt de bankrekening van de katvanger (als verdachte) altijd nieuwe kansen om verdachte transacties en/of contacten inzichtelijk te maken. Die mogelijkheid is er nu nog niet.

13. Schending privacy versus fraude

Om fraude te kunnen voorkomen bij het registreren, is het nodig dat de aanvrager naast NAW gegevens ook zijn/haar Burgerservicenummer opgeeft. Registratie heeft namelijk alleen zin als de gegevens geverifieerd kunnen worden. Maar is de telecomaanbieder wel bevoegd om het BSN te vragen en te registreren? Is dat geen schending van de privacy wetgeving?

Privacy is een afweerrecht dat de persoonlijke levenssfeer beschermt. Het is een ruim begrip: het gaat om de bescherming van persoonsgegevens, de bescherming van het eigen lichaam en van de eigen woning, de bescherming van familie- en gezinsleven en het recht vertrouwelijk te communiceren via brief, telefoon, e-mail.
In Nederland is het recht op privacy vastgelegd in de artikelen 10 tot en met 13 van de Nederlandse Grondwet. Een onderdeel van privacy, de verwerking van persoons-gegevens, wordt sinds 1 september 2001 nader geregeld in de Wet bescherming persoonsgegevens (Wbp).
Naast de Nederlandse wetgeving garandeert ook artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) Let wel: het recht op privacy is niet absoluut; beperkingen op dit recht zijn ingevolge lid 2 van artikel 8 EVRM mogelijk.

Artikel 8 EVRM - Recht op eerbiediging van privéleven, familie- en gezinsleven

1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

In Nederland heeft dit verdrag voorrang op nationale wetgeving.

Er bestaat een spanning tussen privacy en andere belangen, zoals strafvordering en bestrijding van ongewenst gedrag. Voorstanders claimen dat het privacyverlies niet opweegt tegen de voordelen, zoals bestrijding van misdaad en terrorisme.
Privacy betekent dat iemand dingen kan doen zonder dat de buitenwereld daar inbreuk op maakt of weet van heeft. Privacy is vaak onderdeel van ethische kwesties. Ethiek is formeel niet bindend, wetgeving wel. Rechtsnormen zijn echter mede gebaseerd op ethische overwegingen.
Ethiek kan verder gaan dan wetgeving: niet alles wat onfatsoenlijk, dus onethisch is, is onrechtmatig.

[redacted] Immers het kopen van een prepaid telefoon of simkaart berust geheel op vrijwillige basis. Men had net zo goed een abonnement kunnen afsluiten, ware het niet dat een prepaid goedkoper is. Men is al zo gewend aan het fenomeen 'prepaid' dat het gevoel ontstaat dat er iets van je wordt afgepakt. Ongeacht of je aan de doelstelling, het bestrijden van criminaliteit, nu waarde hecht of niet. Ondanks dat het je niets uitmaakt of je wel of niet moet registreren, ben je er toch tegen.
Hoe zat dat vroeger ook weer, toen er nog geen prepaid was? Toen was er geen keus. Je kocht een telefoon met abonnement. Er was niets anders. Wilde je je niet registreren, dan kocht je er geen. [redacted]

[redacted] Blijft na het afwegen van alle voor- en nadelen de weegschaal overwegend in het midden staan, dan kan, in het belang van openbare veiligheid en bestrijding van criminaliteit, art. 8 lid 2 van het EVRM wellicht doorslaggevend zijn.

13.1 Burgerservicenummer

Het Burgerservicenummer (BSN) is een uniek persoonsnummer voor iedereen die ingeschreven staat in de Gemeentelijke Basisadministratie Persoonsgegevens (GBA). Het BSN staat onder andere in het paspoort, op het rijbewijs en identiteitskaart. Het BSN ondersteunt de foutloze uitwisseling van gegevens tussen overheidorganisaties.

Ook met name genoemde organisaties (bedrijven) die verbintenissen met klanten aangaan, waaraan financiële diensten zijn verbonden of waaraan rechten kunnen worden ontleend, willen natuurlijk weten of degene die zich aanmeldt als klant ook daadwerkelijk degene is die hij/zij opgeeft te zijn. Om dit juist en snel en efficiënt te kunnen verifiëren is het Burgerservicenummer noodzakelijk.

In het "*overzicht van organisaties die het Burgerservicenummer gebruiken*" van 6 maart 2013, uitgegeven door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties staat genoemd onder punt 2 "Agentschap Telecom". Het lijkt erop dat dit de telecomaanbieders zijn en dat zij het BSN mogen vragen. Maar dit is niet juist. Dit is een overheidsinstantie / organisatie die zich bezig houdt met de uitgifte- en beheer van radio frequenties en heeft niets te maken met telecomaanbieders (providers)
De telecomaanbieders/providers zijn dus niet bevoegd en/of gerechtigd om naar het BSN te vragen en dit te registreren.

13.2 Proportionaliteit en subsidiariteit

Gezien de "fraude" ervaringen in het buitenland met het registreren van prepaid telefoons, is het uit oogpunt van effectiviteit, noodzakelijk voor telecomaanbieders om het BSN te vragen en te registreren om zodoende snel en zeker de juiste identiteit van de aanvrager te kunnen vaststellen. Zoals eerder vermeldt is het hele systeem van een gedegen registratie afhankelijk van de juistheid en echtheid van de persoonsgegevens. Als blijkt dat men zich zonder problemen kan aanmelden met een valse naam, omdat dit toch niet gecontroleerd wordt, dan is registratie zinloos en werkt het juist contraproductief. Sterker nog hiermee speel je criminelen in de kaart.

Kan de juistheid van de identiteit dan niet op een andere manier worden vastgesteld? Neen. Wanneer iemand zich aanmeldt via de internetsite van de provider, kan de provider nooit weten of die gegevens juist zijn. Zelfs wanneer een kopie van het paspoort wordt gescand en meegezonden (wat overigens onwerkbaar is) is het nog niet zeker dat die persoonsgegevens juist zijn. Het kan immers een vervalst- of gestolen paspoort zijn.
De opgegeven persoonsgegevens (zonder BSN) kunnen ook niet direct door de provider worden gecontroleerd op juistheid. Telecom bedrijven zijn namelijk niet gerechtigd en/of bevoegd om rechtstreeks (online) andere systemen te raadplegen om persoonsgegevens te verifiëren zoals bv het GBA, van de gemeente, het CBR of de politiesystemen. Met andere woorden: verificatie van de persoonsgegevens betekent een lange, moeizame weg. Eerst moet er aanleiding zijn om te twijfelen aan de juistheid van de gegevens. Na deze geconstateerde fraude moet de telecomaanbieder aangifte doen bij de politie. Die rechtsgang moet worden gevolgd. De telecomaanbieder kan uiteindelijk via het proces verbaal de juiste gegevens van de klant achterhalen. Die vorm van verificatie kost veel tijd en menskracht. Gezien de ervaringen met dergelijke procedures (denk aan het opkopersregister) ligt het voor de hand dat de telecomaanbieders het allemaal wel best

vinden en de verificatie achterwege laten. Daarnaast wordt de politie door deze aangiften onnodig belast. Het genoemde scenario is niet bepaald een toonbeeld van efficiëntie en effectiviteit.
TIP: Het is technisch mogelijk om het ingevoerde BSN (en eventuele andere privacygevoelige gegevens) onzichtbaar te maken voor de verwerker. De verificatie vindt dan "onder water" plaats en is na invoer niet meer zichtbaar op het computerscherm.

[redacted]

13.3 Kopietje paspoort

Hoe vaak komt het niet voor dat je bij het aangaan van een verbintenis de verkoper een kopie wil maken van je ID kaart of paspoort? Maar mag dat eigenlijk wel?
Om enige zekerheid te hebben over betaling van abonnementsgelden, kan een telecomaanbieder een krediet waardigheidsonderzoek doen naar een potentiële klant. Daarvoor heeft de ondernemer enkele persoonsgegevens nodig – zoals NAW-gegevens en de leeftijd van de klant in geval van een minderjarige – en kan hij de klant vragen om een geldig identiteitsdocument te tonen om diens identiteit deugdelijk vast te stellen. Zonodig kan de ondernemer de aard van het document en het documentnummer noteren. Het maken van een kopie of een scan is echter niet toegestaan; Op ID kaart en op het paspoort staan je BSN en daar heeft de telecomaanbieder niets mee te maken. Het BSN mag niet door de telecomaanbieder worden verwerkt en ook de pasfoto en andere gegevens op het document zijn voor zo'n kredietwaardigheidonderzoek niet noodzakelijk. In plaats van een kredietwaardigheidonderzoek wordt ook wel de bankpas gecontroleerd en gevraagd om € 0,01 te pinnen om aan te tonen dat de betaalrekening van de nieuwe klant actief is. Het kopiëren of scannen van de bankpas is niet noodzakelijk; door de betaling beschikt de ondernemer immers al over de nodige betaalgegevens, zoals het rekeningnummer en de tenaamstelling van de betaalrekening.
Ondanks dat het niet mag, maken telecombedrijven [redacted] een kopie van een legitimatiebewijs voor hun administratie. Volgens [redacted] s dat nodig om klanten te kunnen identificeren en wordt de kopie bewaard zolang dat voor de overeenkomst nodig is.
Wel zegt [redacted] het BSN-nummer automatisch onleesbaar maakt. Ook [redacted] zijn gevraagd om toelichting, maar zij hebben meer tijd nodig om duidelijk te maken waarom legitimatiebewijzen opgeslagen zijn. Een zegsman van [redacted] stelt het legitimatiebewijs te kopiëren om achteraf discussie over een abonnement te kunnen voeren. Ook is de kopie volgens het bedrijf nodig zodat medewerkers kunnen controleren of zij met de juiste persoon te maken hebben. (bron CBP)

13.4 Asielzoekers en studenten

Maar hoe moet dat straks dan met mensen die geen Burgerservicenummer hebben zoals asielzoekers en studenten die niet in Nederland wonen? De meeste asielzoekers hebben wel een BSN, maar dat staat niet op hun verblijfvergunning en/of rijbewijs, maar wel op hun zorgkaart. (een ID kaart heeft men nog niet). Studenten die niet in Nederland wonen, krijgen een tijdelijk onderwijsnummer. Dit nummer wordt toegekend door de Dienst Uitvoering

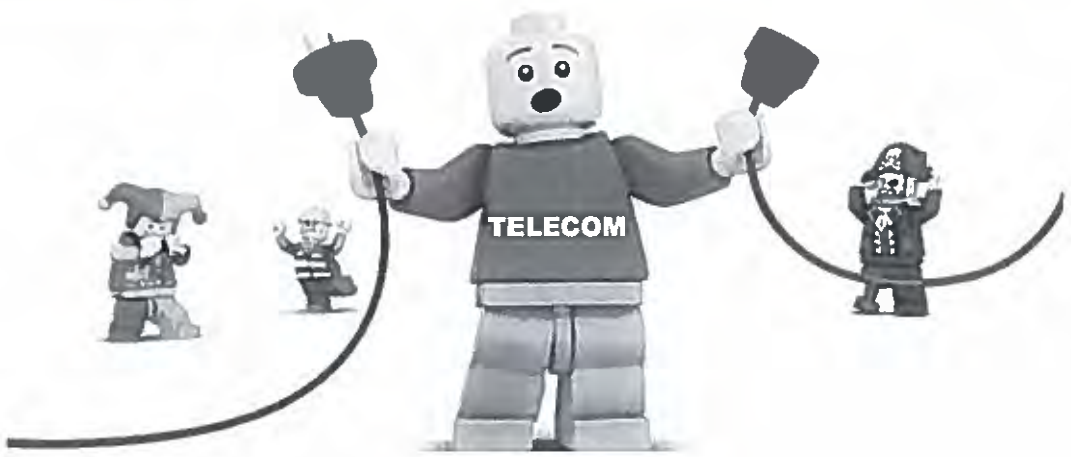
(voorheen IB-Groep). De leerling moet dit tijdelijke nummer weer inleveren op het moment dat hij zich heeft ingeschreven in de Gemeentelijke Basisadministratie Persoonsgegevens (GBA) en een BSN ontvangt van de gemeente.

13.5 Aanmelden / registreren van minderjarige kinderen

[redacted]Jawel, op de aanmeldingssite van de provider moet de mogelijkheid geboden worden dat de wettelijk verzorger (vader, moeder, voogd) zijn minderjarige kind kan aanmelden. De registratie staat wel op naam van de wettelijk verzorger, maar deze kan aangegeven voor wie hij de registratie doet.
Nadere uitwerking van die procedure kan het beste worden gedaan i.c.m. de partners.

14. [redacted]

[redacted]



Technisch gezien lijkt dit geen probleem. Dezelfde infrastructuur maakt het bijvoorbeeld nu mogelijk dat er wel een verbinding tot stand komt en dat het beltegoed wordt afgeschreven. Een simpel filter zal een ongeregistreerde beller niet toelaten op het netwerk.

De prepaid telefoon is bedacht en ontwikkeld voor mensen die weinig bellen en waarvoor een abonnement dus te duur is. Daarnaast is het een prachtig middel om de kosten van "belgrage" kinderen in bedwang te houden. De prepaid telefoon is ervoor om goedkoop te kunnen bellen en niet om anoniem te kunnen bellen.
Uitsluitend als de klant daar zelf aanleiding toe geeft (plegen criminaliteit) worden zijn persoonsgegevens geraadpleegd. En dan ook nog pas na toestemming van justitie.
De voorgestelde adviezen zorgen ervoor dat mensen bewust worden dat men niet langer anoniem is.

[redacted]

De invoering van het project 'IMEI-Blokking' in 2014 is gebaseerd op het blokkeren van het Imeinummer van gestolen of vermiste telefoons, zodat bellen met een gestolen toestel onmogelijk wordt en niemand meer een tweedehands toestel wil kopen, omdat het vanaf dat moment of enige tijd later niet meer zal werken. Het stelen van telefoons heeft geen enkele zin meer. De helingmarkt wordt verstoord.

15. Kostenplaatje

In een normaal businessplan is het belangrijk te weten of de kosten in verhouding staan met het beoogde effect. Maar wanneer de openbare veiligheid en het maatschappelijk belang in het geding zijn mag het kostenaspect niet leidend zijn. [redacted]
Voor hen is het slechts een klein substantieel deel van de omzet. Dit in tegenstelling tot de telecom aanbieders. Zij zullen geconfronteerd worden met hogere kosten. Maar wellicht zijn er oplossingen te bedenken. Voor de rapporteur van dit dossier is onbekend hoe het verdienmodel van de commerciële partners eruit ziet en welke financiële consequenties dit heeft voor de bedrijvigheid.
Voor wat betreft het kostenplaatje voor politie en justitie is de verwachting dat dit onveranderd blijft ten opzichte van de huidige situatie en vermoedelijk zelfs goedkoper zal uitvallen. Ten behoeve van de opsporing wordt door het Ministerie van VenJ jaarlijks een vast bedrag betaald aan de Nederlandse providers. Dat zal door deze maatregelen niet veranderen. Er zijn wel 'geluiden' dat door het vaker opvragen van de zogenaamde 'mastgegevens' er extra kosten door de providers worden gemaakt. [redacted]

Auteur: [redacted]

Bijlage 1

[redacted]

Bijlage 2

CBS jaarcijfers 2010 en 2011 misdrijven

Zie voor de complete tabel:
http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLNL&PA=80344NED&D1=a&D2=0-1,18,42,59-60,69,72-73&D3=0&D4=(l-1)-l&HD=120718-1104&HDR=G2,T&STB=G3,G1

Tabel
Grafiek
Kaart

Regio's	Nederland		
Onderwerpen	Geregistreerde misdrijven		
	Totaal geregistreerde misdrijven	% van totaal geregistreerde misdrijven	Per 1 000 inwoners
Perioden / Soort misdrijf	*aantal*	*%*	*per 1 000 inwoners*
2010	Misdrijven, totaal	1 192 640	100	72,0
	1 Vermogensmisdrijven	703 465	59	42,4
	2 Vernielingen, misdr.openb.orde/gezag	184 310	15	11,1
	3 Gewelds- en seksuele misdrijven	112 695	9	6,8
	4 Misdrijven WvSr (overig)	10 640	1	0,6
	5 Verkeersmisdrijven	152 825	13	9,2
	6 Drugsmisdrijven	17 275	1	1,0
	7 (Vuur)wapenmisdrijven	6 475	1	0,4
	9 Misdrijven overige wetten	4 955	0	0,3
2011*	Misdrijven, totaal	1 192 755	100	71,6
	1 Vermogensmisdrijven	709 995	60	42,6
	2 Vernielingen, misdr.openb.orde/gezag	181 475	15	10,9
	3 Gewelds- en seksuele misdrijven	111 355	9	6,7
	4 Misdrijven WvSr (overig)	11 480	1	0,7
	5 Verkeersmisdrijven	150 960	13	9,1
	6 Drugsmisdrijven	16 745	1	1,0
	7 (Vuur)wapenmisdrijven	7 310	1	0,4
	9 Misdrijven overige wetten	3 445	0	0,2

Bijlage 3 OPTA tabel aantallen en omzet

OPTA Openbaar

Mobiel: Aantal retailaansluitingen

	30-6-2008	31-12-2008	30-6-2009	31-12-2009	30-6-2010	31-12-2010	30-6-2011	31-12-2011
Totaal	19.927	20.627	21.267	20.682	20.599	20.627	21.453	21.848
Postpaid MNO	8.565	9.139	9.750	9.934	9.825	9.983	10.421	10.644
Prepaid MNO	8.391	8.393	8.573	7.628	6.784	6.357	6.423	6.252
Aansluitingen MVNO	2.971	3.095	2.688	2.587	2.702	2.839	2.805	2.933
Met mobiel breedbandinternet					4.410	5.602	6.711	7.646
Specifiek mobiele breedbandinternet aansluitingen			255	533	600	712	943	1.053
M2M					688	736	861	965

Op basis van gegevens van KPN, T-MOBILE en VODAFONE. Op basis van vragen 1_A_2_1-2-4-5-6-7 en 1_B_5_2-7-8 van de SMM.

Bijlage 4 Registrierungsformular

[redacted]

[redacted]

Registrierungsformular

Zur Freischaltung Ihrer SIM-Karte senden oder faxen Sie bitte das gut lesbar ausgefüllte und unterschriebene Registrierungsformular an:

Adresse: [redacted]
Fax: [redacted]

Registrierungsformular

Anrede (Zutreffendes bitte ankreuzen) ☐ Herr ☐ Frau

Vorname, Nachname

Straße, Hausnummer[1]

PLZ, Wohnort

Geburtsdatum[2]

Rufnummer für Rückfragen

E-Mail-Adresse[3]

(SIM-Karte- und Telefonnummer entnehmen Sie bitte dem Anschreiben Ihres ALDI TALK Starter-Sets!)

MEDIONmobile SIM-Kartennummer: MEDIONmobile Telefonnummer:

Hinweis:
Mit der Registrierung erkennen Sie die AGB der E-Plus Service GmbH & Co. KG für Mobilfunkleistungen im ALDI TALK Prepaid Tarif sowie die Leistungsbeschreibung und Preisliste an. ALDI und MEDION handeln im Namen und für Rechnung der E-Plus Service GmbH & Co. KG.

☐ Ja, ich stimme der Verarbeitung und Nutzung meiner Bestandsdaten zur Beratung, Werbung für eigene Angebote und Marktforschung zu.

☐ Ja, ich stimme der Verarbeitung und Nutzung meiner Verkehrsdaten zum Zwecke der Vermarktung und bedarfsgerechten Gestaltung des Dienstes ALDI TALK zu.

Ort, Datum: Unterschrift:

Hinweise/Info:
1) Bitte geben Sie hier eine gültige deutsche Adresse, unter der Sie gemeldet sind an!
2) Eine Registrierung ist erst nach Vollendung des 16. Lebensjahres unter Zustimmung eines Erziehungsberechtigten möglich.
3) Die Angaben sind freiwillig.

ALDI TALK Formulare Registrierungsformular