STEEK NIET ZOMAAR OM HET EVEN WAT IN DE **CLOUD**

# De wazige wereld van datawolken

De cloud wint aan belang in de opslag en de verwerking van persoonsgegevens. De Europese Unie probeert via een nieuwe gedragscode de achterstand op de VS te verkleinen en tegelijk hogere eisen te stellen in databescherming. ***Stijn Fockedey***

Waar staat de informatie over en van de Belg? Veelal is die opgeslagen in 'de cloud'. In de ruime definitie is dat de verzamelnaam voor de talloze datacenters en serverparken die de ruggengraat vormen van het internet. Sommige zaken liggen voor de hand. De Belgische overheid heeft veel gevoelige informatie over haar burgers, zoals belastingaangiftes. De gevoelige aard van de gegevens verplicht de overheidsinstellingen te werken met datacenters in eigen beheer op Belgisch grondgebied. Dat is de enige manier om absolute controle te hebben over de beveiliging. Ook voor banken in België gelden heel strenge regels voor de bewaring van gegevens over klanten. De controle daarop is in handen van de Nationale Bank, die sinds 2011 verantwoordelijk is voor het toezicht op de banken.

Dergelijke gegevens zijn dus makkelijk op een kaartje te plaatsen. Maar hoe zit het met andere data, zoals foto's op Facebook of mails bij Google? "In theorie heb je altijd het recht te vragen waar men uw gegevens opslaat. Maar slechts in zeldzame gevallen zult u een concreet antwoord krijgen", zegt Willem Debeuckelaere, de voorzitter van de Belgische Privacycommissie. Met de antwoorden op de vraag waar men onze data opslaat, bleek inderdaad niet altijd veel aan te vangen. Google, een zeer dominante speler in het onlineleven van de Belg met onder meer de gelijknamige zoekmachine, Gmail en YouTube, antwoordde: "Uw gegevens worden opgeslagen in het Google-netwerk van geografisch verspreide datacentra."

**Amerikaanse aanbieders van clouddiensten en de bijbehorende infrastructuur en software zijn zeer dominant in Europa.**

Uit veiligheidsoverwegingen geven bedrijven liever zo weinig mogelijk vrij waar welke gegevens worden opgeslagen. Zo wil men de kans op pogingen tot hacking en DoS-aanvallen verminderen. DoS (kort voor *Denial of Service*) is een cyberaanval waarbij men het netwerk van het doel overspoelt met trafiek. Dat lijkt een relatief onschuldige vandalenstreek. Maar zo'n aanval ontregelde twee jaar geleden het Nederlandse betaalverkeer. Een DoS-aanval is ook een geliefkoosd afleidingsmanoeuvre om zwakke plekken in IT-infrastructuur te ontdekken.

## Zware beveiliging

"Een goed beveiligd datacenter is zowel fysiek als met technologie sterk beveiligd", zegt Laurens van Reijen van LCL. Het is een van de belangrijkste onafhankelijke uitbaters van datacenters in België. "Maar de beveiliging van data moet ruimer worden gezien dan

**BEWARING VAN DATA**
**Een datacenter moet zowel fysiek als technologisch sterk beveiligd zijn.**

GETT

louter een bescherming tegen diefstal. Tegen accidenteel verlies van data zijn er ook maatregelen nodig. LCL heeft bijvoorbeeld drie onafhankelijke datacenters waar de klant de data kan ontdubbelen. Wanneer een brand, overstroming of een andere ramp een datacenter of serverkamer uitschakelt, dan is de informatie toch volledig beschikbaar omdat die ook nog op andere plaatsen werd opgeslagen."

De werking van de technische installaties wordt gecontroleerd door jaarlijkse audits. Die zijn nodig om aan een strenge ISO-norm te voldoen. "Net door die hoge eisen is er al jaren een trend dat bedrijven hun servers met gegevens verhuizen naar gespecialiseerde datacenters zoals de onze. Het vergt te veel expertise van de meeste bedrijven", vertelt Van Reijen.

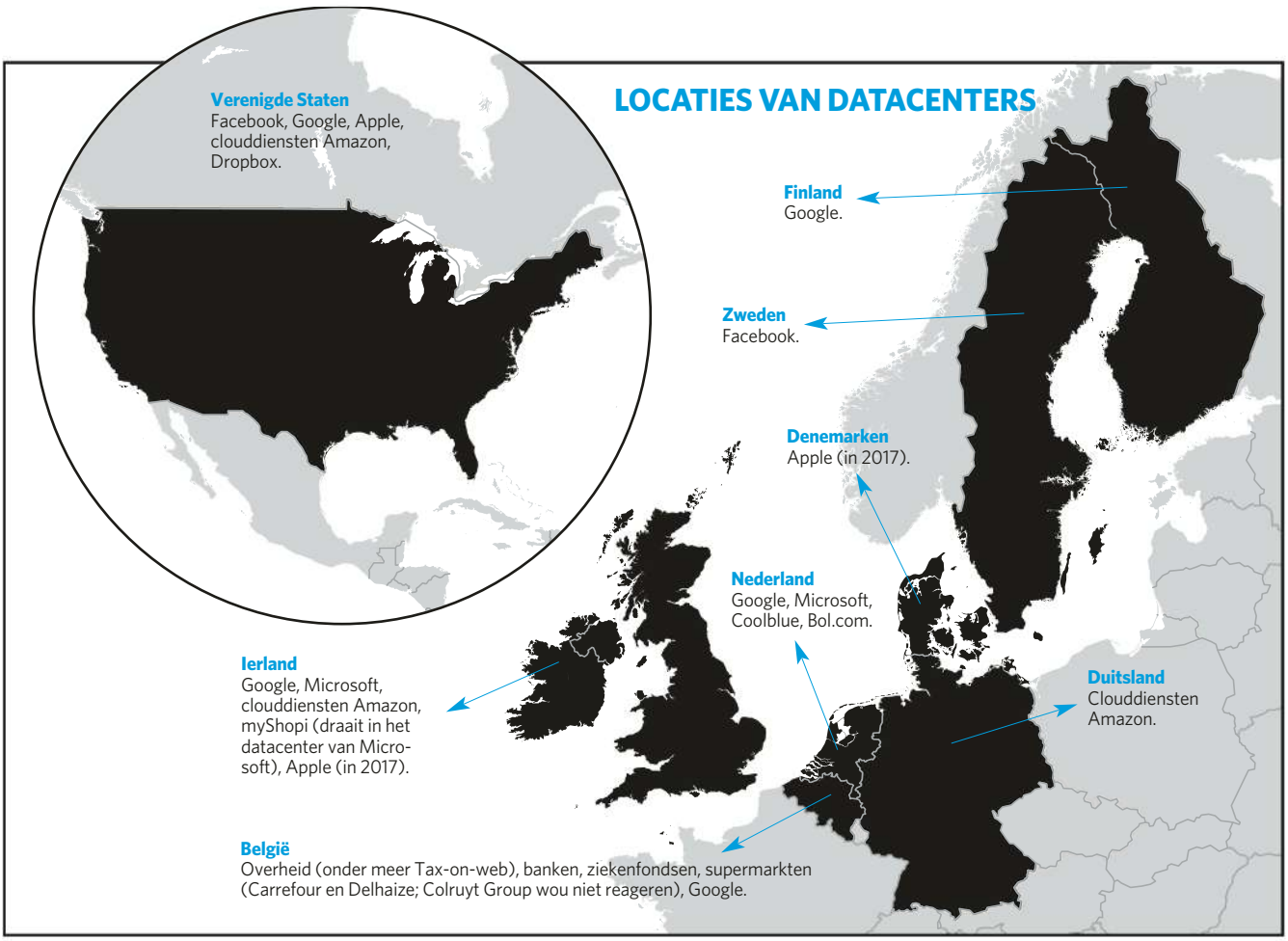
In vergelijking met de VS of Groot-Brittannië zijn Belgische bedrijven relatieve laatkomers in het verhuizen van data en processen naar de cloud. Daardoor ook zijn Amerikaanse aanbieders van clouddiensten en de bijbehorende infrastructuur en software zeer dominant in Europa. De reputatie van Amerikaanse spelers kreeg in 2013 wel een forse knauw, toen klokkenluider Edward Snowden de agressiviteit en de enorme capaciteiten van het Amerikaanse cyberspionageprogramma van het National Security Agency (NSA) onthulde.

**Om die economische belangen te verzoenen met hogere eisen in databescherming, wordt gewerkt aan een gedragscode voor aanbieders van clouddiensten in Europa.**

Bovendien bleken de cyberspionnen ook in staat zwaar beveiligde datacenters in de VS te hacken. Geen enkele computer, geen enkele smartphone, geen enkel netwerk lijkt nog veilig. De Amerikaanse techbedrijven zijn woedend. Toen president Obama in februari een verzoeningsvergadering belegde in Silicon Valley, stuurden de CEO's van Google, Facebook en Yahoo hun kat. Naast imagoschade dreigen Amerikaanse IT- en internetbedrijven ook miljarden dollars aan inkomsten mis te lopen.

## Europese gedragscode

Ook in de Europese Unie zijn de onthullingen van Edward Snowden nog niet helemaal verteerd. Meermaals is al geopperd de *Safe Harbor*-regeling te verstrengen. Dat is een afspraak waarmee Amerikaanse bedrijven beloven zich aan Europese privacy- en databeschermingswetten te houden. In ruil




## WELKE DATA STAAN WAAR?

De data van een Belgische gebruiker worden hoofdzakelijk in Europa en in de VS opgeslagen. Uw data bij de Belgische overheden worden in België gehost, alsook uw gegevens bij de meeste Belgische bedrijven en organisaties. Europese webshops slaan de informatie over hun klanten meestal op in het land waar ze wonen. Facebook, Google en andere grote Amerikaanse internetbedrijven proberen in de regel de data van Europese gebruikers in Europa op te slaan. Hoe dichter de data, hoe sneller. Maar gegevens, vaak kopieën, kunnen ook elders, vooral in de VS, worden opgeslagen. Een uitzondering is Microsoft. Die heeft al jaren een datacenterinfrastructuur opgezet in Ierland en in Nederland, exclusief voor Europese gebruikers.

mogen ze zonder al te veel rompslomp gegevens van Europese burgers verwerken. De nasleep van het NSA-schandaal beïnvloedt ook het Europees beleid in cloudcomputing. De Europese Commissie vreest dat Europa economische groei mist door zijn achterstand in de cloud.

Om die economische belangen te verzoenen met hogere eisen in databescherming, wordt gewerkt aan een gedragscode voor aanbieders van clouddiensten in Europa. Die wordt opgesteld door een stuurgroep waarin ook de aanbieders en andere betrokken partijen zitten. De rapporteur is Hans Graux van het gespecialiseerde ICT-advocatenkantoor time.lex.

"In februari is een voorstel gestuurd naar de Working Party 29 (het overlegorgaan van alle nationale privacywaakhonden, *nvdr*). We verwachten voor het eind van het jaar hun feedback", zegt Graux. "De gedragscode wordt niet opgelegd, maar ze zal wel noodzakelijk zijn voor het halen van een nieuw kwaliteitslabel. En dat wordt niet vrijblijvend. Zware inbreuken kunnen zelfs leiden tot een strafklacht. Los daarvan blijft een risicoanalyse altijd noodzakelijk voor een afnemer van clouddiensten. Men moet altijd goed nadenken welke gegevens men in de cloud stopt. Men mag ook niet met de eerste de beste partij in zee gaan als het om gevoelige informatie gaat." ⊙