

Feitencheck

Cloudwashing

Waarom digitale soevereiniteit met Amerikaanse partners een sprookje is



Excom-lid, algemeen directeur, adjunct-hoofd juridische zaken, hoofd bedrijfs-, externe en juridische zaken: het LinkedIn-profiel van Anton CARNIAUX – achternaam zelfbewust in blokletters – staat vol met titels en functiebenamingen. Zo ziet het profiel van een echte autoriteit eruit. Wat Monsieur Carniaux zegt, heeft gewicht. Zelfs als hij liever zou zwijgen, als hij onder ede staat, als hij moet spreken. Zoals op 10 juni 2025.

Project Bleu, soms ook gewoon Bleu genoemd, is de Franse poging om een soevereine cloud te creëren. Daarop moeten onder andere alle nationale gezondheidsgegevens van Frankrijk worden verzameld. Bleu is een gezamenlijk project. Terwijl Capgemini en Orange officieel als eigenaren worden genoemd, geldt Microsoft slechts als technologiepartner, die een van de wereldwijde Microsoft-cloud geïsoleerde Azure-omgeving moet beschikbaar stellen. Dat moet bescherming bieden tegen extraterritoriale wetten – bescherming tegen de Amerikaanse CLOUD Act. Maar er zijn twijfels over deze bescherming.

En dus werd Monsieur Carniaux op 10 juni 2025 voor een senaatscommissie gedaagd.



Vraag

„Kunt u voor onze commissie onder ede garanderen dat de gegevens van Franse burgers die via de Ugap (Franse centrale inkooporganisatie voor de publieke sector) aan Microsoft zijn toevertrouwd, nooit op bevel van de Amerikaanse regering zullen worden doorgegeven zonder de uitdrukkelijke toestemming van de Franse autoriteiten?“

Iedereen in de EU die zich de afgelopen jaren heeft beziggehouden met gegevensbescherming in de trans-Atlantische betrekkingen, zou het antwoord moeten weten. Het antwoord werd al in 2019 uitgebreid gegeven in een verklaring van het Europees Comité voor gegevensbescherming. Ook bij Microsoft – in de VS, in de EU, in Frankrijk – kende men het antwoord. Maar als Monsieur CARNIAUX het uitsprekt, dan heeft het – dankzij zijn autoriteit – gewicht. Dan verdient het een vetgedrukte kop zoals bij Forbes: **“Microsoft Can’t Keep EU Data Safe From US Authorities”**. Of zoals bij Heise: **“Geen garanties: Microsoft moet EU-gegevens doorgeven aan de VS”**. Of Golem: **“Het sprookje van de Sovereign Cloud”**.



Antwoord

„Non, je ne peux pas le garantir.“ – „Nee, dat kan ik niet garanderen.“

Waarom moest Monsieur Carniaux dit ‘nee’ laten vastleggen? Waarom is digitale soevereiniteit een sprookje? Is er een uitweg? Antwoorden volgen. Oui, naturellement.

Het Amerikaanse Cloudtriumviraat

De drie grote Amerikaanse cloudproviders AWS, Microsoft Azure en Google Cloud domineren de Europese markt, met een gezamenlijk marktaandeel van 70% volgens een recent [onderzoek van Synergy Research Group](#). Hun reclame beperkt zich niet tot de voordelen van bepaalde diensten of technische superioriteit, maar de marketingretoriek lijkt vaak op een loze belofte van soevereiniteit. Zelfs voor een senaat, zelfs onder ede, klonk het aanvankelijk nog als volgt:

„Een ander belangrijk kenmerk is onze sterke betrokkenheid bij de digitale soevereiniteit van Europa en Frankrijk.“

Of zo:

„Het naleven van de voorschriften en het beschermen van de gegevens van onze klanten is voor ons geen optie, maar een verplichting die deel uitmaakt van ons bedrijfsbeleid.“

Het zijn dit soort uitspraken die het volgende ‘nee’ verhullen en het fundamentele probleem systematisch verdoezelen: Europese gegevens zijn nooit beschermd tegen toegang door Amerikaanse autoriteiten, ongeacht waar ze fysiek worden opgeslagen.

En voor deze praktijk van verhullen en verdoezelen bestaat er een passende term: cloudwashing.



De juridische situatie in de VS: het dubbele toegangsprobleem

“Naleving van de voorschriften en bescherming van gegevens ...”. De formulering is slim, want “naleving van de voorschriften” staat voorop. Dat heeft prioriteit, waardoor de bescherming van gegevens slechts een optie wordt als de voorschriften dat toestaan. Er wordt ook niet vermeld om welke voorschriften het eigenlijk gaat. Het klinkt als Europese gegevensbescherming, als AVG, maar in feite zijn het twee Amerikaanse voorschriften die de Europese gegevensbescherming en de Europese soevereiniteit systematisch ondermijnen. Twee voorschriften waaraan Microsoft zich net als de andere Amerikaanse aanbieders moet houden en die uiteindelijk leiden tot “Non, je ne peux pas le garantir”.

1. De CLOUD Act

De Clarifying Lawful Overseas Use of Data Act (CLOUD Act), die in 2018 werd aangenomen, vormt een ongekende breuk met internationale rechtsnormen. De wet machtigt Amerikaanse wetshandhavingsinstanties om Amerikaanse bedrijven te verplichten gegevens vrij te geven, ongeacht waar deze gegevens fysiek zijn opgeslagen of welke lokale wetten hun bescherming voorschrijven.

De reikwijdte van de CLOUD Act is bewust zo breed mogelijk geïnterpreteerd: hij is van toepassing op alle bedrijven die onder de Amerikaanse jurisdictie vallen, met inbegrip van hun buitenlandse dochterondernemingen. Zelfs minimale banden met de VS – zoals het gebruik van Amerikaanse softwarebibliotheken of clouddiensten of samenwerking met een Amerikaanse technologiepartner – kunnen voldoende zijn om een Europees bedrijf aan de CLOUD Act te onderwerpen.

Niemand betwist dat er ernstige misdrijven bestaan waarbij overheidsoptreden ook over de landsgrenzen heen gepast is, maar voor dergelijke gevallen bestonden er al lang vóór 2018 internationale rechtshulpverdragen (Mutual Legal Assistance Treaties, MLAT's). Met de CLOUD Act worden deze verdragen omzeild. In plaats van de diplomatieke weg via officiële kanalen te bewandelen, kunnen Amerikaanse autoriteiten rechtstreeks contact opnemen met particuliere Amerikaanse bedrijven en hen dwingen gegevens vrij te geven, ongeacht waar deze gegevens zich bevinden en wie contractueel gezien de officiële eigenaar is. Er kan zelfs een gag-order worden opgelegd door de rechtbank, waardoor de aanbieders de betrokkenen pas na het verstrijken van een termijn of nooit mogen informeren dat Amerikaanse autoriteiten hun gegevens hebben doorzocht.

2. FISA Section 702

Nog problematischer is sectie 702 van de Foreign Intelligence Surveillance Act (kortweg: FISA 702), die oorspronkelijk was bedoeld voor het surveilleren van buitenlandse agenten, maar in de praktijk kan worden gebruikt voor het massaal verzamelen van communicatiegegevens van alle niet-Amerikaanse burgers. In tegenstelling tot de CLOUD Act, die in ieder geval formeel een gerechtelijk bevel vereist, opereert FISA 702 grotendeels in het geheim. In plaats van een rechtbank treedt de Foreign

Intelligence Surveillance Court (FISC) op. Bezwaren kunnen alleen worden ingediend bij dit orgaan, dat nooit in het openbaar vergadert, en alle procedures zijn permanent vertrouwelijk. Betrokken personen of bedrijven worden niet geïnformeerd over het verzamelen van gegevens of het gebruik ervan.

Mogelijk gebruik: “[Palantir](#) werd in 2003 opgericht met als missie om inlichtingendiensten te helpen beter gebruik te maken van hun gegevens.”

Maar dat is een andere discussie.

AVG-conflicten: juridische grijze zone ondanks adequaatheidsbesluit

Sinds juli 2023 bestaat er met het EU-VS Data Privacy Framework (DPF) een adequaatheidsbesluit van de Europese Commissie voor de VS. Dit maakt het voor gecertificeerde Amerikaanse bedrijven mogelijk om persoonsgegevens uit de EU te ontvangen zonder dat ze aanvullende beschermingsmaatregelen hoeven te nemen. Microsoft, Amazon en Google zijn allemaal gecertificeerd onder het DPF.

Maar [het DPF is niet onomstreden](#): Nadat zowel de “Safe Harbor”-overeenkomst als het “Privacy Shield” door rechtszaken voor het Europees Hof van Justitie waren verworpen, is dit nu de twijfelachtige derde poging van de Europese Commissie om een rechtszeker kader voor gegevensoverdrachten naar de VS te creëren om de economische belangen te behartigen. Het structurele probleem dat tot het mislukken van de voorgangers heeft geleid, wordt hierdoor echter niet opgelost: Amerikaanse bedrijven blijven onveranderd gebonden aan de CLOUD Act en FISA 702. De in het kader verankerde “beschermende maatregelen” – zoals de beperking tot “noodzakelijke en evenredige” gegevensverzameling en de oprichting van een Data Protection Review Court – veranderen niets aan de fundamentele bevoegdheid van Amerikaanse autoriteiten om in het geheim toegang te krijgen tot gegevens.

Ondanks DPF blijft het voor Amerikaanse bedrijven dus verboden om Europese klanten te informeren over FISA 702-gegevensopvragingen. Europese bedrijven kunnen daardoor niet aan hun informatieplicht voldoen, omdat ze zelf niet weten wanneer en in welke mate hun gegevens door Amerikaanse autoriteiten worden opgevraagd.

Het transparantiebeginsel dat in de AVG is verankerd, maakt plaats voor een geheime en potentieel ongegronde gegevensverzameling zonder medeweten of toestemming van de betrokkenen.

Cloudwashing: hoe de grote spelers argumenteren

De bovenstaande uitspraken van Monsieur Carniaux geven een eerste indruk van hoe cloudwashing werkt. In werkelijkheid lijkt er echter sprake te zijn van een uitgekiende strategie, want al jarenlang zijn er een aantal herkenbare patronen die bij alle aanbieders steeds terugkomen:

1. Succesvolle betwistingen van verzoeken van autoriteiten

„We hebben herhaaldelijk bezwaar gemaakt tegen verzoeken van de overheid om klantgegevens die wij te vergaand vonden, en hebben daarbij uitspraken bewerkstelligd die hebben bijgedragen aan het vaststellen van wettelijke normen voor de bescherming van de vrijheid van meningsuiting en de privacy van klanten.“ ([AWS](#))

“[Google](#) beschikt over solide operationele richtlijnen en procedures, evenals andere organisatorische maatregelen ter bescherming tegen onrechtmatige of buitensporige verzoeken van overheidsinstanties om gebruikersgegevens.”

“We hebben meer ervaring met rechtszaken dan enig ander bedrijf als het gaat om het definiëren van de grenzen van overheidsmaatregelen op het gebied van surveillance..” ([Microsoft](#))

Alle drie de spelers gaan prat op hun successen in de rechtbank. Op die manier willen ze een gevoel van veiligheid creëren ten opzichte van willekeurige verzoeken. Dit gevoel is echter bedrieglijk. Niet elk verzoek kan met succes worden aangevochten en zelfs in het kader van de CLOUD Act kan het voorkomen dat betrokken personen hier nooit iets van te weten komen, laat staan dat ze bezwaar kunnen maken – bij FISA 702 is dit zelfs gegarandeerd.

2. De „You control your data“-illusie

„Eigenaar van de data
ben jij, niet Google.“

„You control your data.“

„As a customer,
you control your data.“

Alle drie marktleiders wekken met dergelijke boodschappen de illusie dat klanten daadwerkelijk volledige controle hebben over hun gegevens en dat overheidsinstanties hierdoor geen toegang kunnen krijgen. De realiteit van CLOUD Act en FISA 702 is echter anders. Klanten kunnen weliswaar technische instellingen voor toegang en versleuteling configureren, maar deze mechanismen bieden geen bescherming tegen verzoeken om gegevens van overheidsinstanties. In een dergelijk geval zijn alle aanbieders verplicht om eventuele beschermingsmechanismen te omzeilen.

3. De mythe van de serverlocatie

„To date, we’ve invested billions of euros to expand access to secure, high-performance computing capacity with seven data centers in Europe in addition to 13 cloud regions in Poland, Finland, Germany, Italy, Spain, France, Belgium, Sweden, the Netherlands, Switzerland, and more under development.“ ([Google](#))

„ While [Microsoft](#) Online Services already comply with EU regulations, including GDPR, the EU Data Boundary introduces a more robust, localized approach to data residency, ensuring that Customer Data remains within the EU/EFTA regions.“

“You can choose to store and process your customer data in any one or more of our European Regions.” ([AWS](#))

Alle drie grote Amerikaanse aanbieders maken er intensief reclame voor dat ze datacenters in Europa exploiteren en Europese klanten de mogelijkheid bieden om hun gegevens uitsluitend op Europese servers op te slaan of te verwerken. Deze beloften inzake “data residency” wekken de indruk dat Europese gegevens door hun fysieke aanwezigheid in Europa ook wettelijk beschermd zijn.

Ook dit is een bewuste misleiding. De CLOUD Act maakt expliciet duidelijk dat de fysieke opslaglocatie irrelevant is. De aanbieders zijn zich bewust van deze juridische situatie, maar blijven de Europese serverlocatie benadrukken als een veiligheidsfeature. Daarbij verhullen ze systematisch dat de juridische jurisdictie van het bedrijf, en niet de fysieke locatie van de servers, bepalend is voor de gegevensbescherming.

4. Ondoorzichtige transparantierapporten

Google

“Elke zes maanden publiceren we in een rapport het aantal verzoeken van autoriteiten om gebruikersgegevens en het aantal accounts waarvoor een dergelijk verzoek is ingediend”, belooft Google op de website over het [transparantierapport](#). De meest recente gegevens op het moment van schrijven (augustus 2025) hebben echter betrekking op de eerste helft van 2024. Wat betreft verzoeken in het kader van de CLOUD Act is er veel onduidelijkheid. Wat wel wordt onthuld: wereldwijd waren er 930 Enterprise-verzoeken, waardoor 1007 Enterprise Cloud-kanten werden getroffen. Er is een filter voor landen/regio's. In Duitsland waren er bijvoorbeeld 64 Enterprise-verzoeken, 3 verzoeken om openbaarmaking in noodgevallen en 1 verzoek om bewaring. Er wordt echter niet vermeld hoeveel accounts erbij betrokken waren, noch waar deze verzoeken vandaan kwamen. Het is dus goed mogelijk dat hieronder ook verzoeken op grond van de CLOUD Act zijn opgenomen. Daarnaast zijn er statistieken over juridische verzoeken die via diplomatieke procedures zijn ingediend. Hier kan worden gefilterd op het land dat om ondersteuning heeft verzocht en het land waarvan ondersteuning is gevraagd. De CLOUD Act omzeilt echter precies dit scenario.

De [FISA-verzoeken](#) worden door Google afzonderlijk uitgevoerd en mogen alleen in een bereik worden aangegeven. In de meest recente rapportageperiode (H1 2024) waren er 0-499 verzoeken, waarvan 40500-40999 accounts betrokken waren.



Kort

Verouderde gegevens, giswerk over CLOUD Act-verzoeken, tienduizenden accounts getroffen door FISA 702-verzoeken.

Microsoft

Ook in het [transparantierapport](#) van Microsoft zijn de meest recente cijfers van het eerste halfjaar van 2024. In deze periode waren er 166 verzoeken om gegevens van zakelijke klanten. Hoeveel accounts hierdoor werden getroffen, wordt niet vermeld. Bij één verzoek heeft Microsoft de Amerikaanse wets-handhavingsinstanties inhoudsgegevens verstrekt over een niet-Amerikaanse zakelijke klant waarvan de gegevens buiten de VS waren opgeslagen. De klant was niet gevestigd in de EU/EFTA.

Nog ouder zijn de gegevens over FISA 702, waar de meest recente rapportageperiode betrekking heeft op de tweede helft van 2023. Hier waren er 0-499 verzoeken, waardoor 22.000-22.499 accounts werden getroffen.



Kort

Verouderde gegevens, nadruk op het lage aantal CLOUD Act-verzoeken zonder vermelding van het aantal betrokken accounts, de hoge aantallen [FISA-verzoeken](#) blijven onbesproken.

AWS

Actuele gegevens zijn in ieder geval te vinden bij [AWS](#). In de eerste helft van 2025 waren er 501 verzoeken van Amerikaanse autoriteiten. Daarbij is nooit bedrijfs- of overheidsinformatie buiten de Verenigde Staten openbaar gemaakt.

In deze statistieken zijn de FISA-702-verzoeken, waarvan het aantal tussen 0 en 249 ligt, niet meegenomen. Als we het aantal verzoeken vergelijken met het aantal betrokken accounts bij de andere aanbieders, ligt het vermoeden voor de hand dat ook bij AWS tienduizenden accounts betrokken zijn, maar dat dit verzwegen wordt.



Kort

Benadrukt dat Amerikaanse autoriteiten nooit extraterritoriale bedrijfsgegevens hebben ontvangen in het kader van de CLOUD Act. Volledige geheimhouding van de accounts waarop FISA-verzoeken betrekking hebben.



Datasoevereiniteit als illusie

Datasoevereiniteit betekent volledige controle over eigen gegevens – waar ze worden opgeslagen, wie er toegang toe heeft en onder welke wettelijke voorwaarden ze worden verwerkt. Maar door het gebruik van AWS, Azure of Google Cloud verliezen Europese bedrijven niet alleen de controle over hun gegevens, maar ook de mogelijkheid om deze terug te krijgen. Eenmaal opgeslagen in Amerikaanse cloudsysteem vallen gegevens onder permanente Amerikaanse jurisdictie.

De problemen die hiermee gepaard gaan, zijn talrijk:

1

Geen bescherming tegen industriespionage

Het opslaan van productontwikkelingsgegevens, productieprocessen en klantenlijsten in Amerikaanse clouds betekent dat deze informatie potentieel toegankelijk wordt voor Amerikaanse concurrenten. Dit geldt met name wanneer de concurrentie nauwe banden heeft met de overheid en mogelijk rechtstreeks samenwerkt met de inlichtingendiensten.

2

Geen AVG-compliance

De AVG verplicht bedrijven om betrokken personen te informeren over gegevensverwerking, het doel en de rechtsgrondslag daarvan bekend te maken en de betrokkenen uitgebreide rechten met betrekking tot hun gegevens te verlenen. Amerikaanse surveillancewetten verbieden deze transparantie expliciet. Bedrijven mogen betrokkenen niet informeren over FISA 702-gegevensverzameling en kunnen hen ook geen controlerechten toekennen, aangezien deze door de Amerikaanse wetgeving worden opgeheven.

3

Afhankelijkheid

Je e-mails lopen via Outlook en plotseling verlies je de toegang ertoe. Dat overkwam Karim Khan, de hoofdaanklager van het ISG, nadat hij arrestatiebevelen tegen Israëlische regeringsvertegenwoordigers had verkregen en op de Amerikaanse sanctielijst was terechtgekomen. Microsoft ontkent dat er een verband is. Hetzelfde overkwam de Chinese BGI Group, waarvan verschillende dochterondernemingen op de Amerikaanse sanctielijst staan vanwege het Chinees-Amerikaanse handelsconflict. Sterker nog: ook OneDrive is niet langer toegankelijk. Microsoft zwijgt. Wie de VS een doorn in het oog is, verliest. Een gevaar ook voor Europese bedrijven.

Systematische misleiding als bedrijfsmodel

De Europese gegevenssoevereiniteit is daarbij niet alleen een technische of juridische kwestie, maar ook een kwestie van strategische onafhankelijkheid in een steeds meer gepolariseerde wereld. Wie deze soevereiniteit aan Amerikaanse concerns afstaat, maakt zichzelf kwetsbaar voor chantage en verliest de controle over het meest waardevolle goed van de digitale economie: gegevens.





FAST LTA
Rüdesheimer Str. 11
80686 München
info@fast-lta.de
www.fast-lta.de

Design,
Entwicklung
und Support
in **Deutschland**

