

Europa gaat te traag met beleid voor versleuteling

Behalve voor de Griekse kwestie vormde de Europese schouwburg in Brussel deze week ook weer het decor voor het grootste wetgevingsdebat uit de geschiedenis van de EU. De herziening van de dataprotectierichtlijn uit 1995 sleept zich al drie jaar voort en breekt qua aantal wijzigingsvoorstellen alle Europese records. Vanwege een obsessie met complexe juridische regels mist het debat een robuuste visie op versleuteling. Omdat daardoor de juiste balans tussen privacy en big data nauwelijks besproken wordt, ligt een beleidsdrama op de loer.

Onze informatiesamenleving is steeds meer data-gedreven. Big data, cloud computing en het internet der dingen zijn van nichediscussies voor nerds uitgegroeid tot cruciale thema's voor de toekomst. In recente enquêtes stelt 80-90% van de ondervraagden stevast zich 'ernstige zorgen' te maken over privacy. De huidige richtlijn viert dit jaar zijn twintigste verjaardag en stamt daarmee uit het digitale equivalent van de prehistorie. In 1995 was de Nokia 2110 net gelanceerd, nog zonder het spelletje *Snake* maar al wel met uitschuifbare antenne! Met zulke stokoude wetgeving zijn die 'ernstige zorgen' meer dan terecht. Maar goed, beter veel te laat herzien dan nooit.

In de 'trialoog' van dinsdag onderhandelden de EU-instituten Parlement, Commissie en Raad in Brussel weer over de herziening. Zoals altijd ging het over de complexe contractuele clausules van de algemene voorwaarden waar u en ik steeds toestemming voor geven, voordat een dienst onze data gebruikt. Iedereen weet dat niemand die voorwaarden leest

en gewone 'OK' klikt. Al in 2012 becijferden onderzoekers van Carnegie Mellon dat een gewone internetter daarvoor 76 werkdagen per jaar nodig heeft. Contractuele regeltjes en toestemming werken niet meer. Naast contractuele regeltjes en toestemming zijn vandaag en vooral morgen creatievere oplossingen nodig om de balans tussen privacy en big data te waarborgen.

Versleuteling kent verschillende vormen. Allereerst voor communicatie. Denk aan HTTPS, het slotje in uw browser dat garandeert dat u direct met uw bank communiceert en dat niemand anders de communicatie kan lezen. Ten tweede voor opgeslagen data, bijvoorbeeld uw bankgegevens. Hier wringt versleuteling met big data, want daarvoor moeten data nu nog worden ontsleuteld, wat gepaard gaat met veiligheids- en privacyrisico's. In de nabije toekomst hoeft dat niet meer, vooral na de nieuwste doorbraken in 'homomorphische' versleuteling. Deze nieuwe technieken knippen een databank in ontelbare, onbegrijpelijke stukjes, die verspreid worden over een netwerk van computers; net als bij peer-to-peer technologie, bekend van torrent-downloads. Om te weten waar welk stukje is, gebruikt men een pientere zoekmachine gebaseerd op de 'blockchain', het transactieregister dat ook cryptomunten zonder centrale bank mogelijk maakt, zoals Bitcoin. Zo kun je big data analyses uitvoeren, terwijl

de data op iedere individuele computer versleuteld blijven. Privacy en big data, hand in hand. Momenteel schaalde de technologie nog niet, maar de ontwikkelingen gaan razendsnel. Vooral als slim cryptobeleid deze innovaties steunt.

Versleuteling kent behalve kansen altijd dezelfde bedreigingen voor privacy. Hoe sterk maken we de sleutels en vooral, wie beheert ze? Alleen de gebruiker, of ook de cloudprovider en de overheid? Daarnaast verhuult versleuteling vaak diepere sociale problemen van big data. Moet big data voor gevoelige doeleinden verboden worden? Als het stem-, medisch- of digitale briefgeheim op het spel staat? En waarom is versleuteling, zoals HTTPS, in het post-Snowden tijdperk nog niet verplicht voor alle internetcommunicatie? Waar blijft het onderzoeksgeld voor homomorphische encryptie? Slechts enkele Europarlementariërs agenderen zulke vragen, zoals Sophie in 't Veld van D66. De rest is geobsedeerd door papieren tijgers en het oude denken waar niemand beter van wordt.

De Europese herziening is een historische kans om databeleid naar de toekomst te tillen. De EU moet anticiperen op technologische ontwikkelingen. Een jaar is een mensenleven in technologie, twintig jaar twee tijdperken. Zonder toekomstvisie op de rol van versleuteling in de informatiesamenleving, dreigt voor de Europese privacyherziening eenzelfde lot als in de voortdurende Griekse tragedie. Zodra het politieke akkoord is bereikt, zijn de regels irrelevant geworden.

Axel Arnbak is onderzoeker cybersecurity en informatierecht aan het IViR (UvA) en het Berkman Center (Harvard). Reacties @axelarnbak

Herziening Europese wetgeving biedt historische kans om databeleid naar de toekomst te tillen



Axel Arnbak

