Door Herman Michiel
9 januari 2020

Misschien herinnert u het zich: in april-mei 2018 was er nogal wat zenuwachtigheid bij heel wat bedrijven, administraties, website-uitbaters of internetwinkels, want op 25 mei werd de Algemene verordening gegevensbescherming (AVG) van kracht.

AVG/GDPR

Deze Europese verordening, ook bekend als GDPR (General Data Protection Regulation) heeft als bedoeling de privacy van personen te waarborgen door de verwerking van persoonsgegevens door bedrijven en organisaties strikt te reglementeren [1]. Dit is verre van overbodig, want om allerlei redenen wordt op persoonsgegevens wereldwijd jacht gemaakt. De commercie wil maar al te graag weten of u geïnteresseerd bent in parfums, citytrips of in detectieveromans, beleggersfirma's weten graag waar kapitaalkrachtig volk zit, verzekeringen kunnen uw medisch dossier gebruiken om u de schuld te geven van het incident, de farmaceutische sector kan met dat dossier ook wel wat beginnen, enzovoort, en dan hebben we het nog niet over criminele organisaties. Of over die burgemeester die e-mailadressen, verkregen in het kader van een verkavelingswijziging, voor de verzending van verkiezingspropaganda gebruikte (hij kreeg in het kader van de AVG een boete van 2000 € [2]), of over het onvergelijkbaar veel grotere schandaal over Facebook/Cambridge Analytica. Het is goed dat onze privacy legaal beschermd wordt, het is goed dat de EU zorgt voor een uniforme en grensoverschrijdende regelgeving, want in het digitaal tijdperk zijn onze persoonsgegevens natuurlijk ook in een wip de grens over.

Door de Algemene verordening gegevensbescherming zijn *wereldwijd* alle bedrijven en organisaties gebonden die met persoonsgegevens van ingezetenen van EU-landen omgaan [3]. Gegevens over EU-ingezetenen mogen door een bedrijf in de EU alleen getransfereerd worden naar een derde (niet-EU) land als bepaalde voorwaarden voldaan zijn. In het gunstigste geval (vanuit bedrijfsstandpunt) bevestigde de EU dat de gegevensbescherming in dit derde land voldoende is, d.w.z. vergelijkbaar met AVG ('*essential equivalence*'); het land geniet dan van een zogenoemde '*adequacy decison*'. Is dit niet zo dan moet het bedrijf bij elke gegevensuitwisseling een clausule opnemen, een *Standard Contractual Clause* (SCC), waarbij het verklaart conform AVG te handelen. We laten het aan de lezer over uit te maken of hij/zij zich hierdoor erg beschermd voelt in zijn privacy.

Safe Harbor

Dit is allemaal een beetje ingewikkeld, maar deze wereld is nu eenmaal ingewikkeld. Het wordt echter bedenkelijk als men gaat kijken hoe het gesteld is in het geval van de belangrijkste potentiële misbruikers van onze privacy: de grote cyberspace bedrijven, de *Gang of Four* of GAFA (Google, Apple, Facebook, Amazon). Amerikaanse bedrijven dus die een quasi-monopolie hebben op het dataverkeer,

de online-handel en de datamanipulatie wereldwijd. Gegevensbescherming in de USA is te zwak opdat ze van een *adequacy decison* zou kunnen genieten, en de administratie van de USA heeft zich van meetaf aan verzet tegen Europese 'bemoeiing' met het doen en laten van de grote succesnummers van het Amerikaans kapitalisme. Washington bedong een aparte regeling, afwijkend dus van de Europese standaards. Zo sloot de Europese Commissie met Washington in het jaar 2000 al het *Safe Harbor* akkoord; Amerikaanse bedrijven die zich bij dit akkoord aansloten, zo 'n 4400, konden rustig persoonsgegevens uit Europa naar de USA versluizen. Wat er daarna mee gebeurde heeft de gemoederen in het Brusselse Berlaymontgebouw nooit erg bewogen.

Maar op 6 oktober 2015 verklaarde het Europees Hof van Justitie *Safe Harbor* niet verenigbaar met het Europees recht. Dit was een uitspraak naar aanleiding van een zaak aangespannen door de Oostenrijkse privacy-activist Max Schrems bij de Ierse privacyregulator, wegens het doorspelen van persoonsgegevens door Facebook Ireland aan de moedermaatschappij en bijgevolg aan de NSA. De National Security Agency is de Amerikaanse cyberspionagedienst, dezelfde NSA waarvan bekend werd dat ze de mobiele telefoon van Angela Merkel afluistert. Maar ook van de andere grote high techfirma's is bekend dat ze een open-deurpolitiek hebben met de spionagediensten, en – voor wat hoort wat – dat de Amerikaanse overheid hun schutsengel is die hen behoedt voor de kwaal van de eerlijke belastingen [4]. Onder die omstandigheden moet men weinig illusies hebben dat die overheid streng (of zelfs maar enigszins) zal toezien op de privacyrechten van u en mij.
Het is juist dat in de States zelf enig protest ontstond tegen het gesjacher met de privacy, in die mate zelfs dat high techbedrijven hun blazoen proberen op te poetsen door de vraag naar meer 'transparantie' in het NSA-optreden. Maar zelfs als hiervan iets zou komen heeft het alleen betrekking op Amerikaanse staatsburgers. De privacy van Europeanen en andere bewoners van deze planeet is pasmunt waarmee hun overheden enige goodwill proberen te winnen van de Washington-hegemon.

Privacy Shield

Op het afgeschoten *Safe Harbor* volgde daarom een nieuw akkoord, *Privacy Shield,* dat van de Europese Commissie in februari 2016 de *adequacy decision* kreeg en al in juli van dat jaar in voege trad. Opnieuw een handige regeling voor Amerikaanse bedrijven, want ze moeten slechts een aanvraag doen bij het Amerikaans Ministerie van Handel (DoC) en zich met de *Privacy Shield*-principes akkoord verklaren om een vrijgeleide te krijgen in hun gebruik van Europese privacydata. Omdat het praktisch onmogelijk is voor Europese burgers een klacht in te dienen als ze zich door Amerikaanse bedrijven (of de NSA…) geschaad voelen in hun privacy werd een troostprijs toegevoegd aan *Privacy Shield* : een ombudspersoon die klachten zou onderzoeken. Die ombudsinstantie bleek in de praktijk een papieren bestaan te leiden, en *Privacy Shield* bleek slechts *Safe Harbor* onder een andere naam te zijn.

Privacy-activist Max Schrems en andere verdedigers van het recht op privacy (zoals Privacy International en Access Now) gingen opnieuw in de aanval en opnieuw moet het Europees Hof van Justitie zich uitspreken over de wettigheid van Safe Harbor bis. De uitspraak is nog hangende, maar op 19 december 2019 bracht de advocaat-generaal van dat Hof een advies uit in de zaak 'Schrems 2.0'. Hij had scherpe kritiek op Privacy Shield wegens het gebrek aan bescherming van de privacy [5]; een definitieve uitspraak wordt in de komende maanden verwacht.

Nieuwe Commissie, meer privacy?

Het zal in de nieuwe Commissie von der Leyen zeker niet ontbreken aan commissarissen die zich met digitale materie bezighouden; de privacy-activisten van Access Now tellen er zes! Of dat een zesvoudige garantie is dat er niet langer met persoonsgegevens zal gesjacherd worden is een andere kwestie. Zo is commissaris Thierry Breton (die de gebuisde Sylvie Goulard vervangt) niet alleen verantwoordelijk voor de militaire industrie, maar ook voor de digitale eenheidsmarkt. De geknipte vent voor deze portefeuilles, want deze multimiljonair was tot voor kort *président-directeur général* van ATOS, een bedrijf voor 'digitale dienstverlening', dat naar eigen zeggen "elke dag oplossingen biedt aan militairen en personeel van de binnenlandse veiligheid". Op het gebied van de veiligheid van de privacy van burgers claimt ATOS wel geen speciale competenties. Integendeel, in een interview met Les Echos [6] suggereert hij dat de EU de slag om de persoonsgegevens als commerciële troef verloren heeft van de States en China, maar dat dit niet zal gebeuren voor de datacommunicatie tussen bedrijven (Business to Business of 'B to B').
Een andere betrokken commissaris is Margrethe Vestager, zoals in de vorige Commissie verantwoordelijk voor het concurrentiebeleid en nu ook voor het 'digitaal tijdperk'. Het moet gezegd, Vestager legde Google verschillende miljardenboetes op en kreeg daardoor het aura van onverdroten heldin in de strijd tegen de high tech giganten. Maar die boetes waren omwille van inbreuken op de vrije concurrentie, het watermerk van elk Europees beleid. Als mevr. Vestager dezelfde energie aan de dag legt in de verdediging van de privacy van Europese burgers bieden we haar gratis een column aan op deze site.

Oproep

Het kritisch opvolgen van wat in de EU gebeurt rond privacy, digitale rechten en dergelijke is een taak op zich, al was het maar het opvolgen van wat gespecialiseerde ngo's als Access Now, EDRI, Statewatch, netzpolitik en diverse andere hierover berichten. We hadden het in dit artikel over een paar aspecten van AVG/GDPR, maar ook over de e-privacyverordening, of Passenger Name Record (PNR) en aanverwante dossiers zou er heel wat te zeggen zijn. Wie zich geroepen voelt om hierin bij te dragen gelieve contact met ons op te nemen.

Voetnoten

1. Deze persoonsgegevens hoeven niet noodzakelijk elektronisch (via e-mail bv.) verzameld en gestockeerd te worden, het kunnen ook steekkaarten, microfiches of andere databestanden zijn. Voor de beveiliging van het elektronisch dataverkeer (e-mail...) is er een aparte E-privacyverordening. Over het gelobby rond dit laatste, zie Corporate Europe Observatory (CEO), Big Data is watching you.
2. In het eerste jaar van toepassing van AVG werden in totaal voor 56 miljoen € boetes uitgeschreven, waarvan één van 50 miljoen aan het adres van Google.
3. Ook een aantal niet-EU landen zoals Noorwegen en Zwitserland zijn aangesloten bij AVG.
4. Zie Norbert Häring, US-Regierung verteidigt Google und Co. gegen Besteuerung
5. Zie hierover ook Electronic privacy information center (EPIC), *Data Protection Commissioner v. Facebook & Max Schrems (CJEU)*
6. Les Echos, 7 januari 2020. Voor een korte samenvatting in het Engels, zie Euractiv.