

Remy Chavannes*

Op 3 november publiceerde het kabinet zijn standpunt over het advies van de Commissie Brouwer-Korf, over veiligheid en privacy, en de evaluatie van de Wet bescherming persoonsgegevens.¹ De kop boven het begeleidende persbericht belooft ‘Meer privacy voor burgers’, maar dat dekt niet de lading van de brief. In werkelijkheid gaat de overheid meer gegevens opslaan en uitwisselen. De brief markeert zelfs een fundamentele stap in het denken over veiligheid en burgerrechten. Zij moeten niet meer in concrete gevallen tegen elkaar worden afgewogen; vanaf nu gaat veiligheid voor. Het is een even onjuiste als onnodige keuze.

Dat burgers ‘erop mogen rekenen’ dat overheidsinstanties waar nodig informatie delen, klinkt plausibel, haast evident. Niemand wil dat boeven vrijuit gaan omdat ‘de instanties’ even niet communicerden. Toch is wezenlijk verschil van inzicht mogelijk over wanneer het vanuit veiligheidsoogpunt *noodzakelijk* is dat overheidsorganisaties persoonsgegevens uitwisselen, alsmede over de verdere details van die uitwisseling. Wiens en welke gegevens worden uitgewisseld? Wie kan er allemaal bij? Hoe worden de gegevens geverifieerd en beveiligd? Worden de gegevens vernietigd als verder gebruik niet meer noodzakelijk is voor de veiligheid?

Natuurlijk willen we niet dat een zelfmoordcel niet kan worden afgetapt omdat dat privacyinbreuk zou zijn. Uit het artikel van Dorien Verhulst in dit nummer van *Mediaforum* blijkt dat de Staat op dat punt voldoende bevoegdheden heeft. Evenmin zouden we het aanvaardbaar vinden als een zedenrechercheur een cd-rom met de medische behandelgegevens van alle bekende pedoseksuelen in de trein zou laten liggen. Maar dat men het roerend met elkaar eens kan zijn over makkelijke gevallen, betekent niet dat vooruitgang is geboekt in de discussie over de moeilijke gevallen. In de kabinetsreactie worden over dit soort vragen wel verstandige dingen gezegd, maar door de principiële keuze voor veiligheid boven privacy is het belang daarvan beperkt.

Wellicht onbedoeld biedt de kabinetsreactie een treffende illustratie van het probleem. Het kabinet beoogt een forse uitbreiding van het gebruik van automatische nummerbordherkenning (ANPR), ‘waarbij camera’s op de openbare weg de kentekens van auto’s registreren en deze automatisch vergelijken met bestanden van bijv. openstaande boetes of belastingen. Samenwerking tussen politie en andere overheidsdiensten bij ANPR verloopt aldus veel efficiënter en levert veel meer geld op.’ Ik kan mij voorstellen dat er gevallen zijn waarin automatische nummerbordherkenning een belangrijke bijdrage levert aan het opsporen of voorkomen van een ernstig misdrijf. Als je regels stelt om ervoor te zorgen dat ANPR alleen daarvoor gebruikt kan worden, is er niets aan de hand. Het voorbeeld gaat echter over stelselmatige registratie en opslag van informatie over alle voertuigbewegingen. ANPR is vast een ‘efficiëntere’ manier om wanbetalers te achterhalen. Maar moet de privacy van alle weggebruikers worden geofferd voor efficiencywinst? Het opsporen van mensen met achterstallige boetes of belastingen is in elk geval niet het eerste waar ik aan denk bij ‘de bescherming van veiligheid’. Het feit dat iemand zijn parkeerboete niet heeft betaald, zie ik niet als een geval waarin ‘de veiligheid van individuen concreet bedreigd wordt’, zoals de kabinetsreactie het formuleert.

Laat staan dat registratie en opslag van iedere voertuigbeweging voor het wegnemen van die bedreiging *noodzakelijk* is, in die zin dat het zonder nummerbordherkenning onmogelijk is achterstallige belastingen of boetes te innen. Laat het kabinet dan zeggen wat het kennelijk bedoelt: als privacyregels opsporing op enige manier belemmeren, moeten privacyregels wijken. Als er een opsporingsbevoegdheid denkbaar is die wij nog niet hebben, geef ons die dan. Weg met anoniem prepaid bellen, hier met die meldplicht buitenlandse reisvoornemens, lang leve de bewaarplicht internetverkeer.

De rest van het kabinetsstandpunt is doordrongen van dezelfde instinctieve keuze: ‘veiligheid’ (wat dat ook betekent) vóór ‘privacy’ (in al zijn verschijningsvormen). Dat wil echter niet zeggen dat er verder geen nuttige voorstellen in staan. Meer aandacht voor beveiliging van overheidsdatabases is absoluut noodzakelijk, zeker nu de acute informatieverzamelzucht van de overheid leidt tot steeds meer databases met gevoelige informatie zoals vingerafdrukken, telecomverkeersgegevens, OV-reisgegevens en medische gegevens. Er staat wel meer verstandigs in de kabinetsreactie, vooral over gegevensverwerking door bedrijven. Maar zodra we het ‘veiligheidsdomein’ betreden is de burger zijn zelfbeschikkingsrecht kwijt. Het is duidelijk niet de bedoeling dat de opsporing op enige manier zal worden gehinderd door de aangescherpte privacywaarborgen.

Het kabinet en veiligheidsmensen presenteren het dilemma van privacy versus veiligheid graag als een vals dilemma: veiligheid is een essentieel deel van de persoonlijke levenssfeer, dus schending van veiligheid is ook een vorm van privacyschending. Dat is waar, maar niet erg behulpzaam en geen vrijbrief om dan veiligheidsbescherming categorisch boven privacybescherming te stellen. Je kunt het bovendien net zo goed andersom stellen: daadwerkelijke bescherming tegen ongebreidelde, onzorgvuldige uitwisseling en opslag van persoonsgegevens is een essentieel deel van – en voorwaarde voor – persoonlijke veiligheid.

De keuze tussen veiligheid en privacy is inderdaad een vals dilemma, maar niet omdat privacy eigenlijk een vorm van veiligheid is en je dus altijd voor veiligheid moet kiezen. Het is een vals dilemma omdat het kabinet die keuze tussen bescherming van veiligheid en bescherming van persoonlijke levenssfeer niet in zijn algemeenheid kan, mag en hoeft te maken. De moeilijke, maar enige werkbare aanpak is om per concreet geval een afweging te maken. Als een beleidsvoorstel met negatieve implicaties voor de privacy wordt gerechtvaardigd met een beroep op veiligheid, moet het privacyverlies worden afgewogen tegen de haalbare veiligheidswinst. Uiteraard moeten alle praktische waarborgen worden getroffen om te voorkomen dat meer privacy wordt verloren dan strikt noodzakelijk. Als de realistisch haalbare veiligheidswinst niet opweegt tegen de aan het voorstel inherente privacyschending, moet het kabinet nee durven verkopen aan opsporingsinstanties – en aan burgers uitleggen dat in vrije landen de overheid geen absolute veiligheids garanties kan geven.

* Mr R.D. Chavannes is advocaat te Amsterdam (Brinkhof) en redacteur van dit blad.

1 *Kamerstukken II 2009/10*, 31 051, nr. 5, <https://zoek.officielebekendmakingen.nl/kst-31051-5.html>.