Ons mobieltje gaat verder dan het alziend oog van Orwell

Posted on 14 november 2020 by Coen de Jong

George Orwell voorspelde in zijn boek ‘1984’ een toekomst waarin een dictatoriale staat al zijn onderdanen permanent observeert via teleschermen, die bij alle onderdanen in de huiskamer en op kantoor staan en alles zien en horen. In 2020 hebben we bijna allemaal een smartphone bij ons, waar we ook zijn. Ook de smartphone registreert alles wat we er op doen en weet precies waar we zijn. Is de smartphone een slimmere variant van Orwells telescherm?

Als we niet op onze smartphone kijken dan ligt hij wel binnen handbereik. We regelen bijna al onze contacten met de smartphone en typen, bellen, appen en e-mailen continu. De smartphone is onze agenda, weet wat we vandaag gaan doen, waar we heen gaan of moeten. En we kunnen foto’s en video’s maken, onze stem opnemen in spraakberichten. En we delen eindeloos onze mening, stemming en activiteiten op sociale media.

Iedereen een smartphone

De smartphone onthoudt naar welke internetpagina's we surfen, wat we opzoeken in zoekmachines, welke apps we gebruiken. De GPS in de smartphone houdt permanent bij waar we zijn en waar we heen bewegen. Google Maps houdt bij welke routes we nemen en welke locaties we opzoeken. Daarnaast zend de smartphone permanent signalen uit aan andere apparaten: zendmasten, wifi-routers. Veel smartphones hebben gezichtsherkenningssoftware of een irisscan voor ontgrendeling.

Niet iedereen beseft dat de smartphone ook van alles doorgeeft. Zowel Android, het besturingssysteem van Google dat de meeste smartphones aanstuurt, als iOS van Apple zijn in staat min of meer alles wat op de smartphone gebeurt te monitoren en door te geven aan het moederbedrijf. Sterker nog, zoals Shoshana Zuboff beschrijft in '*The Age of Surveillance Capitalism'*, Android is speciaal ontworpen om data te verzamelen over gebruikers, onder andere via standaard geïnstalleerde apps als Google Maps, Gmail, YouTube en Google Search .

1984 als spookbeeld

1984 is in het politieke discours een vertrouwd spookbeeld, een waarschuwing hoe het niet moet. De vraag is of we er niet al bijna zijn. Orwell's telescherm was een soort televisie, maar dan een die zowel informatie uitzond als opnames maakte. Onze smartphones zijn technisch al tot veel meer in staat. Orwell's hoofdpersoon Winston Smith weet zich vanaf het moment dat hij opstaat in de gaten gehouden. Het telescherm in zijn huis maakt hem 's ochtends wakker, houdt precies bij wat hij doet en voorziet hem van officieel goedgekeurde berichtgeving van de staat.

Ook op zijn werk staan teleschermen die minutieus bijhouden wat hij doet, wat hij zegt tegen collega's en hoe zijn gezichtsuitdrukking staat. Winston Smith weet dat hij altijd moet oppassen wat hij zegt of doet, en dat hij zich altijd bewust moet zijn van zijn gezichtsuitdrukking. Het telescherm is een disciplineringsmiddel van de staat. Ergens is er een centrale meldkamer waarin de agenten van de staat alle onderdanen observeren om dissident of afwijkend gedrag te ontdekken.

De baas over onze smartphones?

Of techniek ons helpt of juist dwarszit hangt sterk af van de mate van controle die we er over hebben. Winston Smith kon de teleschermen in zijn huis of op kantoor niet uitschakelen of ontlopen. Wij kunnen onze smartphone wel wegleggen, uitzetten of niet meenemen. Gebruikers kunnen voor elke app de toegang tot de microfoon en de camera van het toestel uitschakelen. Toch is maar de vraag of de smartphone zich veel van onze instructies aantrekt. Apps kunnen op de achtergrond nog van alles doen en data verzamelen. Controle hebben over wat onze smartphones doen is – zeker omdat zeer weinig gebruikers de techniek en de werking ervan kunnen doorgronden – grotendeels een illusie.

Bovendien: wie kan nog voor langere tijd de smartphone wegleggen of niet gebruiken? Vrienden en familie verwachten dat we online en bereikbaar zijn. En in zakelijk verband kunnen weinig mensen zonder de smartphone-applicaties. De relatie tussen de aanbieder en gebruiker van de applicaties is ongelijk. *Zoom* is al bijna onmisbaar voor thuiswerkers en voor veel instellingen in het hoger onderwijs. Het bedrijf achter Zoom kan bijhouden welke gebruikers met welke andere gebruikers vergaderen en waarover. Het leidde zelfs al tot het blokkeren van Zoom-meetings die de gebruikersvoorwaarden zouden schenden. Opvallend genoeg waren daaronder ook meetings die als onderwerp hadden: censuur van politiek beladen bijeenkomsten door Zoom.

Stel dat uw smartphone doet wat iemand anders zegt

Uw smartphone gaat mee naar werk, vergaderingen en sportactiviteiten. Uw provider houdt gegevens bij – of kan deze terugvinden – over bel- en surfgedrag. En ook in Nederland moeten internetproviders onder de Wet Inlichtingen en Veiligheid meewerken aan verzoeken van politie- en inlichtingendiensten om gegevens af te staan. Berichtenservice WhatsApp – eigendom van Facebook – biedt versleuteling aan van berichtenverkeer, waardoor de inhoud van berichten niet leesbaar is als derden deze onderscheppen. Zoals Kamerlid Kees Verhoeven van D66 onlangs tweette, de ministerraad van de Europese Unie nam onlangs een resolutie aan om deze end-to-end versleuteling (E2EE) te verbieden.

Politiediensten of inlichtingendiensten maken al dankbaar gebruik van

locatiegegevens van smartphones om vast te stellen wie zich waar bevindt, bijvoorbeeld rond Schiphol of andere potentiële doelwitten van terroristen. Of om te zien wie er aan demonstraties deelneemt. En wat als ze van de rechter toestemming krijgen uw smartphone te hacken? Natuurlijk, in Nederland is daar gerede verdenking en gerechtelijke bevelen voor nodig. Maar onder de WIV mogen veiligheidsdiensten heel veel op bevel van hun eigen minister doen, al hebben journalisten en advocaten wat meer bescherming.

En wat als politie en andere diensten besluiten zonder toestemming datagebruik van uw smartphone te gaan verzamelen? Nederlandse inlichtingen- en veiligheidsdiensten wisselen graag gegevens uit met hun Amerikaanse tegenhangers. Google en Apple zijn niet echt in de positie te weigeren als het om een verzoek van de Amerikaanse overheid gaat. Niet voor niets gebruiken criminelen meestal peperdure versleutelde telefoons – voorzien van versleutelde chatprogramma's – die ze regelmatig vervangen.

Privé gedragingen

In een grijs verleden installeerden veiligheidsdiensten microfoons in vaste telefoontoestellen. Dat hoeft niet meer. Een smartphone kan – indien gehacked – instructies krijgen mee te luisteren en kijken en gegevens door te sturen. Uw smartphone bevindt zich doorgaans vlakbij u in uw woonkamer en slaapkamer. Autoriteiten kunnen – desnoods met onder de WIV verplichte medewerking van de provider – gewoon meeluisteren. Google en Apple luisteren soms toch al mee, zo blijkt uit het opnemen van gespreksfragmenten door Google Puur en alleen gebruikt voor scherpstellen van de *voice response*-functie van de Google assistent, zo bezweert Google ons.

Online dating, privé-filmpjes, vragen aan applicaties als Google assistent, ingesproken berichten op de voicerecorder, dicteren van tekst in Microsoft Word, de selfie-camera op uw smartphone. Het genereert data die opgeslagen staan op uw telefoon en die data zijn er af te halen. Commerciële partijen bieden al spyware te koop aan waarmee ouders ongemerkt kunnen meekijken met de chats van hun kinderen op dating-site Tinder. Kwaadwillende actoren zijn natuurlijk prima in staat spyware te verbergen in websites en apps die gokken, seks en drugs aanbieden. En er zijn altijd politici, gezagsdragers en mensen in gevoelige beroepen zich daarmee chantabel maken.

In China is het al gangbaar dat software gedragingen en emoties in de openbare ruimte – kantoren, scholen – registreert, gezichtsuitdrukkingen monitort, micro-expressies en oogopslag bijhoudt. Dat soort software installeert u hier alleen vrijwillig. Voorlopig althans, want voor u het weet is het een feature van veelgebruikte apps en draait het ongezien op de achtergrond mee.

Opsporing verzocht

Veel mensen hebben aan hun smartphone hun vingerafdruk toevertrouwd – om het apparaat te ontgrendelen – en hun identiteitskaart of paspoort ingescand om het Digid te kunnen gebruiken. Allemaal prachtig, zolang deze gegevens alleen benaderbaar zijn voor het doel waarvoor u ze als gebruiker afgeeft. Maar ook dan is nog de vraag welke instanties in welke gevallen deze gegevens kunnen en mogen inzien.

Stemgeluid is uniek. Een vingerafdruk ook. Irisscans ook. Gezichtsherkenningssoftware ontwikkelt zich snel. Onze smartphones zijn in staat deze gegevens te verzamelen en te bundelen. Kennen straks meerdere app-leveranciers uw biometrische gegevens? Google, Apple of wie dan ook kunnen deze gegevens in theorie allemaal opslaan, koppelen en gebruiken voor identificatie. En wat doet dit voor het gemak waarmee instanties mensen kunnen opsporen? In een rechtstaat is dat in elk geval nog met waarborgen omgeven, maar mensen reizen ook – met smartphone en al – naar landen met minder waarborgen.

Politieke profilering

Het is voor Amazon kinderspel om te verzamelen wat u op uw smartphone op Kindle leest, voor Google om vast te stellen wat u op YouTube kijkt en via Gmail de wereld in stuurt, voor Facebook om uw tijdlijn, likes en uitwisselingen met uw vriendkring bij te houden. Waar iemand politiek staat is op basis van zijn zoekgeschiedenis, likes en browse-geschiedenis redelijk goed in te schatten. In elk geval verraad het interessegebieden en de mate van politiek bewustzijn. Facebook maakte ooit een analyse welke facebookgebruikers in Rusland interesse zouden hebben hun land te verraden. Wat zou er gebeuren als zo'n lijst bij de Russische veiligheidsdiensten terecht komt?

Big Tech is maar al te graag bereid informatie te delen met allerlei regeringen

wereldwijd. Freedom House constateerde in 2019 in een rapport getiteld 'the crisis in social media' dat regeringen wereldwijd 90 procent van de internetgebruikers actief monitoren. En dat dit zich niet beperkt tot dictaturen als China. Wie naar de VS vliegt krijgt te maken met een social media achtergrondonderzoek en in het Verenigd Koninkrijk monitorde de politie alleen al in London 9.000 politieke activisten van allerlei achtergronden via geolocatie-tracking en '*sentiment analyse'*. Op basis van data bijeengeschraapt van Facebook, Twitter en andere platforms.

Facebook wordt wereldwijd door regeringen gebruikt om aankondigingen van demonstraties, protest en potentiële opstandigheid van verre te zien aankomen. En om de stemming onder de bevolking te monitoren. Waarbij het vooral gaat om het uitfilteren van potentiële 'lastpakken' en 'radicalen'. Kortom, de social media zijn het perfect spionage-instrument voor machthebbers, maar dan door onszelf collectief vormgegeven.

Cyberveiligheidsdeskundige Arjen Kamphuis zei in 2017 – één jaar voordat hij in Noorwegen vermist werd – dat het bestaan van massasurveillance mensen gedwee en uiteindelijk voorzichtig maakt in het geven van hun mening. Al beseft niet iedereen hoe die surveillance plaatsvind, de wetenschap dat erg veel persoonlijke informatie niet meer echt privé is beïnvloed mensen. In plaats van er tegenin te gaan en op te komen voor het recht op privacy ondergaat men het gelaten en hoopt men op welwillendheid van autoriteiten. Kamphuis gaf het voorbeeld van gebruikers die geen VPN software of Tor-browsers willen gebruiken om hun browsegedrag te anonimiseren omdat ze bang zijn dat overheidsdiensten dat verdacht vinden.

Van collectieve naar individuele observatie

In Orwells wereld van 1984 heerst angst, verbergen mensen gevoelens, kijkt de staat openlijk en zichtbaar mee en bestookt de staat zijn onderdanen met voorgeschreven informatie. Uniformiteit en discipline staan voorop. Het Alziend Oog bestaat in de vorm van een centrale meldkamer die alle burgers in de gaten houdt. De disciplinering door angst zorgt ervoor dat geen onderdaan meer iets durft te ondernemen tegen de almachtige staat.

In onze dagelijkse werkelijkheid geven we via onze smartphone op vrijwillige basis continu persoonlijke informatie door, geven we een groot deel van onze gevoelens prijs, laten we ons (vaak vrij dwingend) informeren via onze eigen bubble en staan

afzondering en conformeren voorop. In plaats van een centrale meldkamer van de Staat is er dataopslag en surveillance door Big Tech. De afhankelijkheid van de eigen smartphone sust burgers in slaap en voorkomt dat mensen elkaar in het echt ontmoeten, waardoor collectieve actie minder makkelijk valt te organiseren.

Collectieve surveillance

Naast angst voor surveillance door autoriteiten via het de smartphone bestaat een andere vorm van in de gaten houden: de collectieve surveillance online op sociale media. Waar alles en iedereen elkaar de maat neemt en labelt. Waar alsmaar striktere spraakcodes ontstaan en een opiniepolitie actief is. Waar oude tweets en berichten uit het niets opduiken om mensen mee zwart te maken. En waar zich een scheiding in twee kampen die elkaar fanatiek bestrijden aftekent: de 'Deugmensen' tegen de 'Populisten'.

Dit Alziend Oog van de sociale media heeft overal *Inoffizielle Mitarbeiter*, de term die de Oost-Duitse geheime dienst Stasi hanteerde voor burgers die andere burgers in de gaten hielden. Iedereen kan zijn vrienden, buren en kennissen aangeven op sociale media. Het is een telescherm zonder centrale meldkamer van de Staat maar met een collectieve meld- en ondervragingskamer. Weinig ontsnapt aan de aandacht van dit Alziend Oog. Een uitspraak, een retweet of een gedeelde link kunnen de trigger zijn om een publiek tribunaal op gang te brengen.

Zelfcensuur

Daarbij komt de wildgroei aan sociale media codes op werkplekken en onderwijsinstellingen. 'Pas op, het ligt gevoelig in jouw positie' is een veelgehoord advies. Hoe lager in de organisatie een medewerker staat, hoe dwingender dat advies van de werkgever meestal is. Dat bemoeienis van werkgevers en onderwijsinstellingen met de uitingsvrijheid van personeel en studenten tegen de geest van de grondwet ingaat dringt amper nog door.

Stel dat in de eerste helft van de 19e eeuw Nederlanders met een opleiding (leraren, vakbondsleiders, ambtenaren en juristen) ook niets 'gevoeligs' hadden gezegd en gevonden van de toenmalige machtsverhoudingen. Hadden we dan ooit een beweging richting democratie gekend in Nederland?

Onzekerheid versterkt zelfcensuur. Als mensen weten dat wat ze online doen in de

gaten loopt maar het tegelijk het onduidelijk is welk soort uitingen precies tot problemen kan leiden. Mensen nemen het zekere voor het onzekere en passen hun gedrag online aan als ze angst ervaren om hun mening te uiten. Burgers veranderen dan in pratende robots die voor het telescherm een show opvoeren en hun gezicht in de plooi houden.

Leven in een vissenkom?

We leven onder vrijwel permanente observatie van bedrijven als Google, Facebook en Apple. Ja, er zijn waarborgen en wetten en privacy-regels. Maar zelf zijn wij niet in staat te verifiëren of Big Tech zich daar aan houdt. Wel weten we op basis van hun gedrag uit het verleden dat ze de grens graag oprekken.

Overheden zouden Big Tech aan banden kunnen leggen. Maar overheden werpen ook een begerig oog op al die informatie in de datapakhuizen van Big Tech. Nu zijn het 9000 activisten in Londen, straks zijn er wellicht meer categorieën 'lastpakken' die via de smartphone op de radar komen. De teleschermen van nu zijn mobiel, geïndividualiseerd en vele malen geavanceerder dan Orwell kon voorzien. Maar het basisprincipe had hij perfect beschreven.