Auteur: mr. A.IJ. (Ard) Ruiter werkt als privacy- en beveiligingsfunctionaris/senior inspecteur bij de ILT Inlichtingen- en Opsporingsdienst (ILT-IOD). Hij schreef dit artikel op persoonlijke titel en is bereikbaar via LinkedIn.

Vooruitzien met cyber- en datasecurity

Over informatiebeveiliging en de algoritmetoezichthouder in het coalitieakkoord 2021

Op de dag dat het kabinet-Rutte III al elf maanden demissionair was, presenteerden de partijleiders van VVD, D66, CDA en ChristenUnie het coalitieakkoord met de titel 'Omzien naar elkaar, vooruitkijken naar de toekomst' (1). Een wereld zonder ICT-voorzieningen en zonder de steeds voortschrijdende digitalisering, is inmiddels ondenkbaar. Op welke wijze geeft de nieuwe, oude coalitie invulling aan de eisen van informatiebeveiliging en cybersecurity?

Na de Tweede Kamerverkiezingen op 15, 16 en 17 maart 2021 startte de onderhandelingen voor een (nieuwe?) coalitie met de aanstelling van twee verkenners. Eén verkenner werd op 25 maart 2021 gefotografeerd met notities, waarop onder andere de inmiddels zeer bekende frase was aangetekend: 'Omtzigt, functie elders'. Dit had betrekking op het Kamerlid dat zich in de maanden daarvoor had vastgebeten in de zogenoemde Kinderopvangtoeslagaffaire, waarover het kabinet viel. Het veroorzaakte een kettingreactie waar we de gevolgen nog steeds van merken, ook uit het oogpunt van informatiebeveiliging. Dit voorval zette de formatie op zijn kop en werd uiteindelijk hét politieke moment van 2021. De interne informatie had vrij gemakkelijk beveiligd kunnen worden en had nooit op straat mogen komen te liggen.

Op 17 november 2021 schreef De Volkskrant over een soort 'proeve van een regeerakkoord' dat een 'betrokkene bij de formatie' in de trein had laten liggen. Met enige schaamte werd opgebiecht wie dat was. Daaraan kon je zien dat de awareness zeker wel aanwezig is, maar geen mens onfeilbaar is (2). Na de langste coalitieonderhandelingen uit de vaderlandse parlementaire geschiedenis is er dan voor de kerst nog overeenstemming. Met in de titel een tautologie: vooruitkijken is immers altijd gericht op de toekomst. Voordat we kijken wat er in dit document staat over informatiebeveiliging en cybersecurity, bezien we even wat op Duits federaal politiek niveau is gebeurd.

IT-beveiliging: cyber- en datasecurity

IT-beveiliging krijgt steeds meer aandacht. Informatiebeveiliging omvat zowel cyber- en datasecurity. Cyber- en datasecurity zijn van oorsprong twee verschillende disciplines. Ze liggen in elkaars verlengde en worden vaak met elkaar verward, maar kunnen elkaar zeker versterken. Cybersecurity omvat het bredere spectrum van beveiliging van data en IT-systemen tegen diefstal, verstoring of misbruik van hardware, software of data. Cybersecuritymaatregelen zijn ontworpen om dreigingen tegen netwerksystemen en applicaties te bestrijden, ongeacht of deze dreigingen van binnen of buiten een organisatie komen. Datasecurity gaat over de bescherming gedurende de gehele lifecycle van digitale informatie tegen bedoelde of onbedoelde aanpassing, verwijdering, diefstal of openbaarmaking van data door ongeautoriseerde personen.

Duits akkoord: 178 pagina's

In Duitsland verliepen die onderhandelingen in 2021 wat sneller. Ook in de Bondsrepubliek waren namelijk recent parlementsverkiezingen. Onze oosterburen schreven in ruim twee maanden een akkoord onder de titel: 'Durf meer vooruitgang te boeken: verbond voor vrijheid, gerechtigheid en duurzaamheid', dat uit maar liefst 178 (!) pagina's bestaat. Het Duitse akkoord vermeldt het woord 'informatiebeveiliging' ('IT-Sicherheit') elf keer, de Algemene Verordening Gegevensbescherming (AVG) ('Datenschutz-Grundverordnung' (DSGVO) vier keer en heeft een separate paragraaf over digitale burgerrechten en informatiebeveiliging. 'Het uitbuiten van zwakke punten in IT-systemen staat in een zeer problematische verhouding tot informatiebeveiliging en burgerrechten', aldus het Duitse coalitieakkoord. Zo wordt geschreven over het instellen van een recht op encryptie, een effectief beheer van kwetsbaarheden, met als doel om beveiligingslacunes te dichten, en de specificaties 'security-by-design/default' in te voeren. Tevens wordt gesproken over anonimiseringstechnieken, het creëren van rechtszekerheid via normen en het overschrijden daarvan moet gaan leiden tot strafrechtelijke aansprakelijkheid bij illegale deanonimisering. Ook wordt de ambitie uitgesproken om het MKB te ondersteunen in de ongecompliceerde promotie en ondersteuning voor informatiebeveiliging, AVG-conforme gegevensverwerking en het gebruik van digitale technologieën (3).

Nederlands akkoord: 55 pagina's

Na bijna negen maanden onderhandelen in Nederland in 2021 was er dan eindelijk de 55 pagina's tellende overeenstemming. Deze tekst kent de woorden 'informatiebeveiliging' en 'information security' niet één keer; 'cybersecurity' staat er twee keer in. 'Privacywetgeving' wordt niet genoemd in de paragraaf over digitalisering, maar in die over gezondheid. De digitale revolutie met nieuwe technologieën biedt kansen, maar zij brengt ook een breed scala aan nieuwe vraagstukken met zich mee: 'De huidige digitale revolutie biedt geweldige kansen voor onze samenleving en economie. Die kansen gaan we benutten met uitstekende digitale vaardigheden, een sterke Europese digitale markt, hoogstaande digitale infrastructuur en ambitieuze samenwerking in technologische innovatie. Tegelijkertijd zorgt digitalisering voor een digitale kloof en groeiende ongelijkheid in onze samenleving. Ook onze veiligheid, rechtsstaat, democratie, mensen- en grondrechten en concurrentievermogen staan onder druk. Dat vraagt om solide spelregels, toezicht en strategische autonomie.'

De citaten uit het coalitieakkoord die gerelateerd (kunnen) zijn aan informatiebeveiliging:

- Wetenschap, bedrijfsleven, 'startups', 'scale-ups', kenniscoalities en overheid slaan de handen ineen om de kansen die digitale technologie biedt te verzilveren. We stimuleren innovatie en investeren in chips- en sleuteltechnologieën zoals kunstmatige intelligentie en quantumcomputing.
- We pakken (in Europees verband) de marktmacht en datamacht van grote tech- en platformbedrijven aan om de concurrentiepositie van bedrijven en de privacy van burgers te verbeteren.
- Nederland wordt het digitale knooppunt van Europa en krijgt robuust, supersnel en veilig internet in alle delen van het land.
- We nemen het voortouw en zetten in Europees verband in op versterking van de samenwerking tussen lidstaten op het gebied van digitalisering, onder meer op mensgerichte inzet van kunstmatige intelligentie, digitale ethiek, ontwikkeling van digitale identiteit en cybersecurity en 'open source'.
- Iedereen krijgt de kans om mee te komen door digitale kennis- en vaardigheden aan te bieden in het onderwijs en via om- en bijscholing. We pakken digibetisme gericht aan via een publiek-private strategie voor digitale geletterdheid en we verbeteren de toegankelijkheid van digitale overheidsdiensten, met behoud van alternatieven voor digitale overheidscommunicatie.
- We willen dat inlichtingendiensten beter in staat zijn om hun slagkracht te benutten en hun capaciteit uitbreiden om nieuwe en toenemende digitale dreigingen en aanvallen assertief op te sporen en te bestrijden, met waarborgen voor goed en effectief toezicht en digitale burgerrechten.
- We beschermen onze bedrijven, vitale infrastructuur en economisch kapitaal beter door centraal gecoördineerde structurele samenwerking tussen onder andere het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC), overheden, bedrijven en wetenschappers. Zij kunnen sneller en makkelijker informatie delen over digitale kwetsbaarheden en 'hacks'.
- Cybercriminaliteit zoals 'ransomware' is zeer ondermijnend. We investeren daarom in een brede meerjarige cybersecurity aanpak en in cyberexpertise bij de politie, rechtspraak, het Openbaar Ministerie (OM) en defensie.
- We erkennen fundamentele burgerrechten online. We versterken daarom veilige digitale communicatie en passen geen gezichtsherkenning toe zonder strenge wettelijke afbakening en controle. We investeren in een sterke positie van de Autoriteit Persoonsgegevens en versterken samenwerking en samenhang tussen de diverse digitale toezichthouders. We regelen wettelijk dat algoritmes worden gecontroleerd op transparantie, discriminatie en willekeur. Een algoritmetoezichthouder bewaakt dit. De overheid geeft het goede voorbeeld door niet meer data te verzamelen en onderling te delen dan nodig en ontwikkelt regels voor data ethiek in de publieke sector.
- We geven mensen een eigen 'online' identiteit en regie over hun eigen data.
- We beschermen kinderen (...en...) geven ze het recht om niet gevolgd te worden en geen dataprofielen te krijgen.
- Iedereen blijft eigenaar van de eigen gezondheidsgegevens. Gegevens- en data uitwisseling tussen patiënt/cliënt en aanbieder en aanbieders onderling wordt, conform privacywetgeving, verbeterd waarbij uniformiteit noodzakelijk is.
- We zorgen dat toezichthouders als de Autoriteit Persoonsgegevens (...) extra middelen krijgen om hun taken goed te kunnen uitvoeren.
- We maken afspraken met het bedrijfsleven en overheden over het stimuleren van thuiswerken.
- Hyperscale datacentra leggen een onevenredig groot beslag op de beschikbare duurzame energie in verhouding tot de maatschappelijke en/of economische meerwaarde. Daarom scherpen we de landelijke regie en de toelatingscriteria bij de vergunningverlening hiervoor aan.
- We versterken de expertise van de aanpak van cybercriminaliteit in alle delen van de strafrechtketen.
- We zorgen ervoor dat de grondslagen voor die gegevensuitwisseling met de juiste waarborgen, zoals doelbinding en proportionaliteit, zijn verankerd in de wet en dat in adequaat toezicht is voorzien.
- We stimuleren de vrije en veilige uitwisseling van ideeën en borgen de academische vrijheid van wetenschappers. We stellen kaders vast voor de wetenschappelijke samenwerking met onvrije landen. 'Open science' en 'open education' worden de normen, mits de nationale veiligheid hierbij niet in het geding komt.
- We zetten in op open strategische autonomie van de EU en stimuleren innovatiekracht en slimme industriepolitiek. Zo worden we leidend in digitalisering en nieuwe technologieën.
- We versterken onze specialismen in 'cyber' en inlichtingen. Dit gebeurt in nauw overleg met onze belangrijkste partners (bij de Defensieparagraaf).
- We maken afspraken met het bedrijfsleven en overheden over het stimuleren van thuiswerken.

De AP is opgericht en aangewezen als toezichthouder op de naleving van de wettelijke regels voor bescherming van persoonsgegevens.

Algoritmetoezichthouder

De coalitie gaat 'cyber' en inlichtingen bij Defensie versterken, en zet zich ervoor in dat inlichtingendiensten beter in staat zijn om hun slagkracht te benutten en hun capaciteit uitbreiden om nieuwe en toenemende digitale dreigingen en aanvallen assertief op te sporen en te bestrijden. Dat moet zijn omgeven met waarborgen voor goed en effectief toezicht en digitale burgerrechten. Er zal wettelijk worden vastgelegd dat algoritmes worden gecontroleerd op transparantie, discriminatie en willekeur. Een algoritmetoezichthouder moet dit gaan bewaken.

De algoritmetoezichthouder – onthoud die naam, het kan nog van pas komen bij het scrabbelen – wordt inmiddels ook al 'algoritmewaakhond' (4) genoemd en moet 'fundamentele burgerrechten' online beschermen. De nieuwe toezichthouder wordt ondergebracht bij de Autoriteit Persoonsgegevens (AP) en moet volgens plannen van het kabinet de transparantie van algoritmes bewaken en zorgen dat ze niet discrimineren of willekeurig zijn. Het aanstaande kabinet wil daarnaast investeren in de AP en de 'samenwerking en samenhang tussen de diverse digitale toezichthouders' versterken. Welke organisatie de coalitie rekent tot de 'diverse digitale toezichthouders', wordt niet helder; daarover is echter wel een uitgebreide beschrijving (5).

De AP is opgericht en aangewezen als toezichthouder op de naleving van de wettelijke regels voor bescherming van persoonsgegevens, waaronder de AVG, de Uitvoeringswet AVG (UAVG), de Wet politiegegevens (Wpg), de Wet justitiële en strafvorderlijke gegevens (Wjsg) en de Wet basisregistratie personen (Wet BRP). De taken van de AP bestaan onder andere uit: toezicht, klachtafhandeling, advisering, voorlichting en internationale taken. De budgettaire bijlage bij het coalitieakkoord vermeldt dat de separate algoritmetoezichthouder een budget krijgt van 3,6 miljoen euro per jaar. De extra gelden voor de AP bedraagt in 2023 één miljoen euro, in 2024 twee miljoen euro, in 2025 drie miljoen euro en vanaf 2026 structureel 3,6 miljoen euro, bovenop de 25 miljoen euro die de AP al krijgt. Vanaf 2022 moet de AP volgens een KPMG 2020-prognose groeien van 184 naar 470 voltijdsbanen om alle taken 'goed uit te kunnen voeren' (6). In dat onderzoek werd ook gekeken naar de doelmatigheid en doeltreffendheid van de AP en naar mogelijkheden om efficiënter te werken. De minister voor Rechtsbescherming schreef in zijn Kamerbrief van 19 november 2020: 'Geconstateerd is dat de AP nog altijd een organisatie in opbouw is. Een aantal functies zijn nog niet ingevuld, de automatiseringsgraad is laag en haar bedrijfsvoering staat nog in het begin van ontwikkeling. Volgens accountants- en adviesorganisatie KPMG is het aannemelijk dat er op termijn door leereffecten, procesoptimalisatie, investeringen in automatisering (zoals de invoering van een zaakvolgsysteem) en investeringen in de bedrijfsvoering efficiënter gewerkt kan worden. Daarnaast kan meer datagedreven en risicogericht gewerkt gaan worden. Het oppakken van risicoanalyse en effectmeting moet leiden tot een efficiëntere en effectievere uitvoering. Hier valt in de toekomst veel winst te behalen (6)." Recent berichtte de Nationale ombudsman in zijn rapport 'Voor een dichte deur', dat de AP niet goed omgaat met privacyklachten van burgers en het lijkt zelfs dat de AP de klachten voornamelijk afhoudt (8).

De kritische lezer kan opmerken dat nog niet bekend is wanneer de algoritmetoezichthouder er daadwerkelijk moet zijn en welke wettelijke bevoegdheden deze toezichthouder precies krijgt, wat er onder algoritme moet worden verstaan en

wat de reikwijdte van deze autoriteit zal zijn. Houdt ze toezicht op enkel overheidsorganen of ook op publiek-private partnerships, op (wetenschappelijke) onderzoeksinstituten, particuliere ondernemingen of wellicht internationaal opererende private bedrijven? Komt er toezicht op de algoritmen of op datgene wat een algoritme verwerkt? Als een algoritme persoonsgegevens verwerkt, dan ligt het toezicht nu al bij de AP. Bij andere vormen van data-analyse en dataverwerking waarbij geen persoonsgegevens in het geding zijn, ligt het toezicht bij instanties als het Agentschap Telecom of bij de Autoriteit Financiële Markten zolang het financiële gegevens betreft. Waarschijnlijk zal de nieuwe autoriteit gaan opereren op het snijvlak van consumentenbescherming, data- en gegevensmanagement, behoudt van de 'online' identiteit, het zelfbeschikkingsrecht over privacy- en persoonsgegevens en wellicht nog andere domeinen die door het gebruik van algoritmes geraakt worden. Het Duitse coalitieakkoord vermeldt dat: 'Voor een betere handhaving ('Durchsetzung') en coherentie van gegevensbescherming willen we voor de toepassing van de privacybescherming bindende besluiten mogelijk maken.' Dus hier rijst ook de vraag welke tanden, standvastigheid en bijtkracht de Nederlandse waakhond krijgt. Algoritmes moeten natuurlijk vooraf, heel voorzichtig worden vormgegeven, op basis van de waarden en normen die wij in dit land belangrijk vinden.

In het nieuwe kabinet zal een bewindspersoon speciale aandacht hebben voor digitalisering; net zoals in het huidige kabinet is dat de staatssecretaris van Binnenlandse Zaken en Koninkrijkrelaties.

Bekijk het eindverslag van de informateurs en het coalitieakkoord op de site van het Bureau woordvoering kabinetsformatie 2021 op: https://www.kabinetsformatie2021.nl/actueel/nieuws/2021/12/15/aanbieding-en-toelichting-eindverslag-en-coalitieakkoord

Uitwerkingen

De uitgangspunten in het coalitieakkoord zullen nog moeten worden uitgewerkt. De verwachting is dat de nieuwe bewindslieden deze uitwerkingen samen met de Voorjaarsnota in de Tweede Kamer zullen behandelen. De volgende Tweede Kamerverkiezingen staan gepland voor 2025, tenzij die vervroegd worden. Kortom, het nieuwe kabinet heeft tweeëneenhalf jaar om die plannen in daden om te zetten. Binnen de samenleving en alle organisaties vinden ontwikkelingen plaats die te maken hebben met het toenemend gebruik van ICT, digitale informatie, data- en informatiesystemen. De transitie van het computertijdperk naar het datatijdperk is volop gaande waarbij aandacht komt voor de positie van de burgers, de veilige en betrouwbare informatie en een (duurzame) innovatie. Data wordt gezien als een belangrijke aanjager voor innovatie. Er zijn daarbij volop uitdagingen rondom privacy, (data- en cyber) security, ethiek en compliance. Ook burgers/ klanten kunnen vanwege de technologieën steeds meer zelf doen: geen werkprocessen in organisaties, maar video-on-demand, in het weekend zakendoen met de bank via internet en op dinsdagavond nog even een aanvraagformulier voor een overheidsdienst invullen. De behoefte aan gespecialiseerde vakmensen wordt steeds groter: van IT-monteurs tot data/cybersecurityspecialisten.
Er is dus werk genoeg; een mooi vooruitzicht, niet?

Referenties

(1) https://zoek.officielebekendmakingen.nl/blg-1009826; bijlage bij Kamerstukken II, 2020/21, 35788, nr. 77

(2) https://www.volkskrant.nl/nieuws-achtergrond/lees-het-hier-zelf-de-proeve-van-een-regeerakkoord-van-vvd-en-cda~b4ea4d75/

(3) 'Mehr Fortschritt wagen; Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit', Koalitionsvertrag
2021-2025 zwischen der SPD, BÜNDNIS 90/ DIE GRÜNEN und den FDP, Berlin, 2021, p. 15-19: https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800

(4) https://www.nrc.nl/nieuws/2021/12/15/nieuw-kabinet-wil-algoritmewaakhond-oprichten-a4069035

(5) Zie voor een overzicht van de toezichthouders: Bijlage 3 bij de kabinetsbrief van 20 april 2020 over de Initiatiefnota 'Menselijke grip op algoritmen' en het onderzoek 'Toezicht op gebruik van algoritmen door de overheid', Kamerstukken II, 2019/20, 35212, nr. 3.

(6) https://zoek.officielebekendmakingen.nl/blg-957075

(7) Kamerstukken II, 2020/21, 25 268 en 32 761, nr. 192

(8) Nationale ombudsman 'Voor een dichte deur: Een onderzoek naar hoe de Autoriteit Persoonsgegevens omgaat met ongenoegen van burgers over de behandeling van privacyklachten', rapportnr.: 2021/139, Den Haag: 21 december 2021
https://www.nationaleombudsman.nl/system/files/bijlage/Nationale%20ombudsman%20-%20Rapport%20Autoriteit%20Persoonsgegevens%20Voor%20een%20dichte%-20deur.pdf