Agentschap Telecom
Ministerie van Economische Zaken
en Klimaat

European Commission

Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (033) 460 08 00
F (033) 460 08 50
www.agentschaptelecom.nl

Agentschap Telecom Reactie Openbare raadpleging

Van
M. Vrieze

T

Datum
14 juli 2021

AI Act Agentschap Telecom Feedback

Algemeen
Agentschap Telecom is de autoriteit in het digitale domein en is de uitvoerder en toezichthouder op digitale infrastructuur in Nederland en heeft met interesse kennisgenomen van het voorstel "Artificial Intelligence Act" (hierna: AI Act) van de Commissie. In 2020 heeft AT in de publieke consultatie op het White paper on artificial intelligence – "A European approach to excellence and trust" van de Commissie gereageerd, het is goed om te constateren dat aandacht is besteed aan onze punten. De inhoud van de AI Act sluit goed aan bij een groot deel van onze werkvelden, zoals continuïteit, cybersecurity en weerbaarheid van veilige apparaten, beschikbare telecom & infrastructuur.
AT waardeert het initiatief van de EC voor de AI Act en vindt het voorliggend voorstel een goede basis voor verdere ontwikkeling van normen voor AI-systemen. Heldere normen zijn nodig om als autoriteit te kunnen toezien op veilig en betrouwbaar gebruik van algoritmen. Het adresseert de juiste risico's en maakt de juiste risico indeling (deels verbieden, deels controle en deels transparantie eisen). Ook de keuze om bij (High Risk) AI-systemen vereisten te introduceren voor markttoegang is een verstandige keuze.

We hebben de AI Act beoordeeld en vragen aandacht voor aspecten die van invloed zijn op een transparante en eenduidige markttoegang, effectief toezicht en het borgen van een Europees level playing field bij de inzet en het gebruik van AI-systemen in de samenleving. Deze zijn:

- Scope: digitale wereld en fysieke wereld;
- Relatie andere EU-wetgeving;
- Definities;
- Standaardisatie en conformiteit;
- Bevoegdheid (nationaal en internationaal);
- Coördinatie tussen toezichthouders;

- Rechtsbescherming burgers.

Het doel is hiermee bij te dragen aan het maatschappelijk vertrouwen in het gebruik van AI. We lichten deze aspecten in onderstaande paragrafen toe.

1. Scope

De AI Act maakt geen duidelijke koppeling tussen het fysieke domein en het digitale domein. AI is gedefinieerd als een softwaresysteem maar in het begrip 'High Risk AI-systemen' worden de 'safety components' van een product ten behoeve van fysieke veiligheid van personen en bezittingen aangeduid. Terwijl bij AI-systemen in het digitale domein juist de veiligheid *door de werking of het gebruik door (AI) software* wordt bepaald. De koppeling tussen de domeinen kan gemaakt worden door een verwijzing op te nemen in de AI Act naar aanpalende regelgeving als de NISD[i] en eIDAS[ii], het ontbreken daarvan bemoeilijkt de analyse van overlap of gaten in de regelgeving.
Daarnaast zijn veel AI-systemen afhankelijk van het functioneren van een digitale infrastructuur, dus een verwijzing naar de kaders die de betrouwbaarheid van die infrastructuur behartigen ligt voor de hand (NIS, Telecomcode).

2. Relatie andere EU-wetgeving

Met de opzet van de verordening sluit de Commissie aan bij al bestaande Europese regelgeving, in het bijzonder die regelgeving waarin de digitale veiligheid van producten, diensten en processen wordt gereguleerd. Tegelijkertijd roept de wijze waarop dit gebeurt vragen op over de onderlinge verhouding tussen met name de RED[iii], CSA[iv], NISD en de AI-verordening. Zou de Commissie kunnen aangeven hoe de verschillende Europese wet- en regelgeving op het gebied van digitale veiligheid in elkaar grijpt en met elkaar samenhangt?
Voorbeelden van samenhang:

- RED: Radio Apparatuur is volgens artikel 6 lid 1 geen High Risk terwijl te veel uitgestraald vermogen wel een gevaar voor de gezondheid kan vormen. Het radioapparaat (zoals een mobiele telefoon) kan aangestuurd worden door AI (bij 5G en 6G bijvoorbeeld) maar omdat het geen safety component betreft, lijkt het buiten de scope van de AI-verordening te vallen. Het is onvoldoende helder of de AI-software die het apparaat aanstuurt onder het AI framework valt, onder de RED, of geen van beide;
- NISD: Er is bij de High Risk definitie gekozen voor een meer beperkte scope van 'critical infrastructure' dan de bij NISD, namelijk; "supply electricity and water, heating and operation of road security". De ononderbroken levering van deze diensten en de integriteit ervan vormen het risico voor de maatschappij, niet de 'safety components' die de installaties of werknemers beogen te beschermen. Onduidelijk is of de AI-systemen in de 'operation en management' van deze essentiële diensten onder de NISD of het AI framework vallen.
- CSA: In artikel 41 lid 2 van de verordening wordt verondersteld dat High risk AI-systemen die een CSA conformiteitsverklaring hebben en voldoen aan een van de CSA certificeringsschema's, ook voldoen aan de cybersecurity vereisten zoals beschreven in artikel 15 van de verordening. De CSA kent echter drie 'assurance' niveaus waarop cybersecurity certificering kan plaatsvinden, te weten basic, substantial en high. De

keuze voor het niveau van certificering vindt onder de CSA plaats door de producent. Wij vinden het wenselijk dat in de AI Act goed wordt vastgelegd hoe de CSA assurance levels passen bij High Risk definitie.

3. Definities

De uitleg van definities heeft verstrekkende gevolgen voor de toepasselijkheid van wetgeving en bevoegdheid van de toezichthouders. Toezichthouders zijn bij heldere definities meer voorspelbaar en aanbieders en gebruikers ontlenen er zekerheid aan. Het is belangrijk meer aandacht te besteden aan het aanscherpen van de definities of het nader duiden daarvan. We noemen drie voorbeelden:

- eIDAS: Het gebruik van de term 'remote biometric identification system' in het AI framework lijkt een andere betekenis te hebben ten opzichte van andere toepassingen (o.a. identificatiesystemen voor eID en AML Anti money laundering toepassingen) waar gesproken wordt van 'remote identification' in de eIDAS verordening;
- Productregelgeving: Het begrip "provider" sluit niet aan bij productregelgeving. Net zomin als "small-scale provider" of "user". Deze verwijzen eerder naar diensten dan producten.
- "Producenten van (High Risk) AI-systemen": Voor de vraag wie de producent is van een AI-systeem moet duidelijk zijn of een CE-markering gekoppeld wordt aan het doel van het product. Wie is bijvoorbeeld de producent van het AI-systeem in een slimme speaker?

4. Standaardisatie en conformiteit

Standaardisatie draagt bij aan harmonisatie van de markttoegang door onder andere producten en diensten veilig, compatibel en uitwisselbaar te maken, waarmee het maatschappelijk belang wordt gediend. Tevens heeft standaardisatie en normering een belangrijke rol bij het uitoefenen van de handhaving- en toezichtstaak op nationaal niveau. De systematische en getrapte indeling van geharmoniseerde standaarden -en bij het ontbreken van deze standaarden- het kunnen stellen van aanvullende vereisten is in de concept Verordening Artificiële Intelligentie helder verwoord.
Voor een consistente en systematische opzet van mogelijk aanvullende vereisten op het terrein van AI -en in bredere zin digitale veiligheid-is het goed dat de Commissie vroegtijdig de Europese Standaardisatie Organisaties (ESOs) en ENISA actief heeft betrokken. De ESO's hebben de kennis en expertise om een belangrijke rol te kunnen vervullen bij de verdere ontwikkeling van standaarden en voor ENISA geldt dit bij de identificatie van relevante ontwikkelingen bij AI binnen de CSA certificering als ook bij de inrichting van het systeem van conformiteitsbeoordeling. Wij adviseren daarom de rol van de ESOs bij de ontwikkeling van standaarden te borgen in de verordening.

5. Bevoegdheid (nationaal en internationaal)

Het is onduidelijk welke 'competent authority' wanneer kan/mag/moet acteren.

- Een AI-systeem dat op de markt is gebracht kan door meerdere gebruikers in meerdere lidstaten gebruikt worden. Hoe voorziet de EC een coördinatie van toezichtsactiviteiten en een efficiënte aanpak van de handhaving als meer dan één sectorale toezichthouder bevoegd is, en

mogelijk ook meerdere lidstaten bevoegd zijn ten aanzien van één provider?
- Is jurisdictie verbonden aan de vestigingsplaats van de provider, producent of gebruiker? Welke lidstaat is bevoegd om tot handhaving over te gaan, is nog onvoldoende scherp. Meer duiding of aanscherping is gewenst.

6. Coördinatie tussen toezichthouders

- Gedeelde verantwoordelijkheden betekent dat in de verschillende fasen van het toezicht de bevoegde autoriteit zaakkennis moet overdragen of dat een organisatie te maken krijgt met meerdere toezichthouders. Hoe wordt informatiedeling en coördinatie van toezichtsactiviteiten voorzien? En wat is de juridische basis?
- Daarnaast vraagt effectief markttoezicht in Europa om naast nationaal toezicht een Europees netwerk op te richten waar aan gezamenlijke toezichtsactiviteiten, onderzoeken en handhaving wordt gewerkt.

7. Rechtsbescherming burgers

Er is onvoldoende voorzien in de mogelijkheid voor burgers om individuele problemen met AI te rapporteren, waardoor de bescherming tekortschiet. Op basis van de AI Act kijkt een toezichthouder naar het AI-systeem en de werking in het geheel, niet naar de gevolgen voor een individueel geval. Om de burgers voldoende rechtsbescherming te bieden moeten zij kunnen aangeven dat zij zijn benadeeld door de toepassing van AI.

Het maatschappelijk vertrouwen in AI-toepassingen is afhankelijk van rechtsbescherming, effectief toezicht, transparante markttoegang en standaardisatie.

---

[i] NISD. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[ii] eIDAS. VERORDENING (EU) Nr. 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

[iii] RED. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment.

[iv] CSA. VERORDENING (EU) 2019/881 VAN HET EUROPEES PARLEMENT EN DE RAAD van 17 april 2019 zake ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie.