Geachte leden van de verkiezingsprogramma commissie,

Met deze brief vragen Amnesty, Bits of Freedom, Open State Foundation, SETUP en Waag u om in het verkiezingsprogramma van uw partij voor de Tweede Kamerverkiezingen op 22 november 2023 aandacht te besteden aan de volgende (digitale) kwesties:

Algemeen

- Digitalisering moet in het volgende kabinet een hoofdzaak worden met voldoende slagkracht. Dat betekent dat er een minister van Digitale Zaken moet komen die in de ministerraad op alle onderwerpen met een digitaal component kan meepraten en beslissen. Organiseer specifieke ambtelijke domeinkennis m.b.t. digitale zaken op alle departementen.
- Onze digitale overheid van de toekomst is open-by-design en minimaliseert de data die zij verzamelt. Dit bevordert rechtszekerheid, veiligheid en flexibiliteit. Het draagt bij aan het verkleinen van onze afhankelijkheid van Big Tech. Dat betekent dat het nodig is om digitale standaarden te verplichten, de inzet op open source software te vergroten en open data als uitgangspunt te nemen.
- Investeer in lokale journalistiek voor een divers medialandschap en een sterke democratie. Een vitaal journalistieke controle is nodig om toezicht op de politiek te waarborgen, zowel centraal als binnen decentrale overheden. Daarvoor is het essentieel dat ook de lokale redacties en journalisten hun werk goed kunnen uitvoeren. Het versterken van de lokale journalistiek is belangrijk voor een gezonde democratie en een divers medialandschap.
- Besteed 2% van het budget voor ICT-activiteiten van de Rijksoverheid aan maatschappelijk betrokkenheid bij het ontwerp en eventuele realisatie van deze ICT-systemen.
- Leerlingen verdienen betere bescherming van hun privacy. Leerlingvolgsystemen kunnen negatieve gevolgen hebben op de ontwikkeling en mentale gezondheid van leerlingen. Geef als Rijksoverheid, in navolging van het dwingende advies over mobieltjes de klas uit, een soortgelijk advies over ziekmakende leerlingvolgsystemen.

Uitingsvrijheid

- Er is al veel geregeld rondom de bescherming tegen online haat, doxing, bedreigingen en laster én de bescherming van uitingsvrijheid. Toch ontbreekt het mensen vaak aan handelingsperspectief. De overheid doet soms teveel en soms te weinig. Mensen moeten zichzelf kunnen verweren tegen online bedreigingen en laster, tegelijkertijd moet de overheid zich strikt houden aan de wettelijke (on)mogelijkheden en moet de overheid extra aandacht hebben voor kwetsbare groepen zoals kinderen of minderheden én voor vormen van problematische uitingen waar zij tot nu toe weinig oog voor had, zoals pesten.

Encryptie

- De vertrouwelijkheid van online communicatie is essentieel voor de bescherming van mensenrechten en voor de bescherming van onze digitale infrastructuur. Het kabinet handhaaft

daarom haar standpunt dat het onwenselijk is om de ontwikkeling, de beschikbaarheid en de toepassing van encryptie in te perken. Het kabinet blijft dit internationaal uitdragen.

Surveillance

- De overheid mag alleen experimenteren met nieuwe technologie wanneer daar robuuste mensenrechtenwaarborgen voor bestaan. De politie experimenteert niet met ingrijpende technologie als gezichtsherkenning of drones zonder duidelijke wettelijke basis en onafhankelijk toezicht. Onze vrije samenleving is geen levend laboratorium.
- Bescherm mensen tegen onrechtmatige online surveillance. Mensen moeten vrij zijn om online hun mening te uiten zonder bespied te worden door de politie, gemeenten of de NCTV.
- Respecteer mensenrechten bij de inzet van surveillancetools rondom demonstraties. Onrechtmatige surveillance kan mensen afschrikken van demonstreren, terwijl dat juist zo belangrijk is in een vrije democratische samenleving.
- Partijen zetten zich er voor in dat gezichtsherkenning en andere vormen van biometrische massasurveillance in de openbare ruimte wordt verboden.

Kunstmatige Intelligentie en algoritmen

- Er zijn nog te veel incidenten met AI- en algoritmetoepassingen die discrimineren, of andere schendingen van mensenrechten tot gevolg hebben. De controle van, en het toezicht op dergelijke systemen wordt verzwaard, in lijn met Europese wetgeving als de AVG en de AI Act.
- De overheid moet zich inzetten voor een sterke toezichthouder op toepassingen van kunstmatige intelligentie en zorgt voor de benodigde bevoegdheden en middelen.
- Het algoritmeregister van de Nederlandse overheid wordt verplicht gesteld voor algoritmen die worden gebruikt in de publieke sector. Er komt geen uitzondering voor algoritmen die worden gebruikt voor handhavingsdoeleinden.
- Overheidsinstellingen zien af van het gebruik van zelflerende algoritmen als het gaat om a) besluitvorming met rechtsgevolgen, b) besluitvorming en handelingen die de rechten en vrijheden van individuen aantasten en/of c) besluitvorming en handelingen die een grote impact hebben op de samenleving.
- In situaties waarin het gebruik van algoritmen grote impact kan hebben op mensen, bijvoorbeeld bij de opsporing van fraude in het sociale zekerheidsdomein, zien overheidsinstellingen af van het gebruik van black box-systemen.
- Er komt een bindende en verplichte mensenrechtentoets voor algoritmen die worden gebruikt in de publieke sector. De mensenrechtentoets wordt zowel door de ontwikkelaar als gebruiker van een AI-systeem uitgevoerd. Het uitgangspunt wordt dat de mensenrechtentoets openbaar wordt gemaakt.
- Er komt een verbod op het gebruik van afkomstgerelateerde gegevens, zoals nationaliteit en etniciteit, in risicoprofielen die bedoeld zijn voor het opsporen van potentiële normovertreders of mogelijke verdachten van strafbare feiten of fraude.

AVG/privacy

- De Rijksoverheid neemt een actieve rol in het prioriteren van de naleving van de AVG bij overheidsinstellingen en stelt daarvoor de nodige middelen ter beschikking. Uit verschillende onderzoeken is immers gebleken dat de AVG door de overheid nog slecht wordt nageleefd.[1]

Geheime diensten

- Nederland zorgt, in lijn met Conventie 108+ (internationaal verdrag voor gegevensbescherming), voor bindend en effectief toezicht, juist wanneer de gegevensverwerking plaats vindt in het kader van nationale veiligheid. Immers: hoe ingrijpender de bevoegdheid en de context, hoe strenger het toezicht zou moeten zijn.[2]
- Cyberwet: Het wetsvoorstel voor de Cyberwet wordt aangepast, zodat geheime diensten de enorme hoeveelheden gegevens die ze verzamelen, zo snel mogelijk moeten blijven beoordelen op relevantie.[3]
- In de Cyberwet moet een verbod worden opgenomen op de uitwisseling met het buitenland van gegevens die zijn verzameld met de snapshotbevoegdheid, en dus ongezien zijn.

Economie

- De inkoop door de overheid moet transparanter, vanaf het vaststellen van inkoopbeleid tot en met de gunning en evaluatie. Dit draagt bij aan de kwaliteit en een goede verantwoording, het voorkomen van ongewenste buitenlandse inmenging en bescherming van mensenrechten. Denk hierbij aan de inkoop van AI systemen, digitale surveillance middelen en grondstoffen.
- Transparantie over jaarverslagen van bedrijven moet verplicht worden, ook voor brievenbusfirma's. Handelsregisters worden zo open mogelijk. Dit betekent dat de privacy van ZZP'ers beschermd moet worden door ze als aparte categorie op te nemen en los te koppelen van de categorie eenmansbedrijven. Misbruik van bedrijfsconstructies, verborgen 'ultimate benifical owners' en geheime belastingdeals vergroten de kans op fraude, faciliteren belastingontwijking en belemmeren de strijd tegen de financiering van terrorisme.

Platformen

- De overheid zet zich in voor een sterke implementatie van de Digital Services Act en Digital Markets Act. Dat houdt onder andere in dat er een sterke toezichthouder is, de ACM, die voldoende middelen heeft.
- Nederland zet zich in voor verdere regulering van online platformen (binnen de EU) die ertoe moet leiden dat ons communicatielandschap diverser wordt en we niet vastzitten aan monopolistische markten en de mechanismen van Big Tech. Voorbeelden daarvan zijn het aanpakken van aanbevelingssystemen en op tracking gebaseerde advertenties en het stimuleren van interoperabiliteit en open protocollen.
- De overheid investeert in een digitale publieke infrastructuur die afhankelijkheid vermindert van bestaande leveranciers die publieke waarden met voeten treden.

[1] https://www.bitsoffreedom.nl/2023/05/25/wat-is-er-allemaal-gebeurd-sinds-ons-onderzoek-naar-gemeenten/
[2] https://www.bitsoffreedom.nl/2023/03/15/bindend-toezicht-is-wel-zo-chique-en-wel-zo-duurzaam/
[3] https://www.bitsoffreedom.nl/2023/01/17/er-woedt-een-machtsstrijd-om-jouw-gegevens

Openheid en transparantie

- Het lobbyregister - waar een Kamermeerderheid een voorstander van is - moet worden doorgevoerd. Dit is nodig om (de schijn van) belangenverstrengeling tegen te gaan en vertrouwen in de politiek terug te winnen. Met de invoering van een lobbyregister krijgt iedereen inzicht in de lobbycontacten van bewindspersonen. Hiermee wordt de aandacht voor een gelijk speelveld bevorderd. Ook geeft Nederland hiermee opvolging aan de aanbeveling van GRECO en kritiek van de Europese Commissie om corruptie aan te pakken.
- De Wet open overheid (Woo) is inmiddels meer dan een jaar van kracht, maar de implementatie loopt achter. Er is geen eenduidigheid gecreëerd, vanuit Den Haag moet meer ondersteuning komen in de vorm van richtlijnen en adequate budgetten. De overheid moet prioriteit geven aan het op orde brengen van haar informatiehuishouding, zodat het kan voldoen aan het recht van burgers om inzicht te krijgen in publieke informatie. Het overschrijden van termijnen bij het beantwoorden van Woo-verzoeken mag aan het eind van deze regeringsperiode niet meer voorkomen.

Hoogachtend,

Dagmar Oudshoorn

Directeur, Amnesty International Nederland

Lotje Beek

Beleidsadviseur, Bits of Freedom

Serv Wiemers

Directeur, Open State Foundation

Jelle van der Ster

Algemeen Directeur, SETUP

Sander van der Waal

Research Director, Waag