COMMISSION DE LA JUSTICE

du

MARDI 8 NOVEMBRE 2022

Matin

_____

COMMISSIE VOOR JUSTITIE

van

DINSDAG 8 NOVEMBER 2022

Voormiddag

_____

De behandeling van de vragen en interpellaties vangt aan om 12.14 uur. De vergadering wordt voorgezeten door mevrouw Kristien Van Vaerenbergh.
Le développement des questions et interpellations commence à 12 h 14. La réunion est présidée par Mme Kristien Van Vaerenbergh.

01 Vraag van Kris Verduyckt aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen, de Culturele Instel.) over "Slimme brillen" (55029807C)
01 Question de Kris Verduyckt à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments, des Instit. Culturelles) sur "Les lunettes intelligentes" (55029807C)

01.01 **Kris Verduyckt** (Vooruit): Mijnheer de staatssecretaris, slimme brillen zijn een nieuw product op onze Belgische markt en doen mij enigszins de wenkbrauwen fronsen. Het product is ontwikkeld door Meta, het bedrijf achter Facebook, samen met Ray-Ban. Die bril stelt de gebruiker in staat om te filmen en die filmpjes op te slaan. Dat gebeurt op een manier waarop het voor een derde persoon niet echt heel duidelijk is dat die gefilmd kan worden. Het beste bewijs daarvoor is dat Meta grote advertenties heeft geplaatst om mensen te verwittigen van het feit dat die brillen in omloop zijn.

Daarin zitten volgens mij enkele ingrediënten die grondrechten in gevaar brengen. Het is namelijk bijzonder moeilijk om ervan uit te gaan dat iedereen het zomaar leuk vindt om gefilmd te worden. Bovendien zijn ongewenste toepassingen mogelijk. Zo kan iemand worden gefilmd terwijl hij geld afhaalt bij een geldautomaat. Dat heeft natuurlijk negatieve gevolgen.

Mijnheer de staatssecretaris, hoe beschouwt u dergelijke producten? Hebt u in dat verband al contact gehad met de Gegevensbeschermingsautoriteit? Kunnen er voorwaarden worden verbonden aan het gebruik of de verkoop van dergelijke brillen?

Hoe bekijkt u het aspect dat producenten het blijkbaar zelf nodig vinden om sensibiliseringscampagnes voor hun eigen product op te zetten om consumenten te verwittigen?

01.02 Staatssecretaris **Mathieu Michel:** Geacht Kamerlid, verschillende fabrikanten werken aan de ontwikkeling van slimme brillen die volgens sommige, zoals Nokia, uiteindelijk smartphones zullen vervangen.

Van belang in het geval van die slimme brillen is dat de huidige wetgeving reeds bepaalde regels oplegt. Allereerst wil ik eraan herinneren dat het filmen van een herkenbaar persoon een verwerking van persoonsgegevens impliceert, die in beginsel moet voldoen aan de voorwaarden van de AVG en de privacywet. Behalve in bepaalde omstandigheden, zoals de specifieke context van een politieonderzoek, staat de wetgeving algemeen het filmen of fotograferen van mensen zonder hun medeweten niet toe.

In het geval van het gebruik van slimme brillen is het dus verboden om mensen stiekem te filmen. De AVG vereist immers de toestemming van de gefilmde persoon en richt zich op het hogere belang van de gefilmde persoon om zijn privacy te respecteren.

De gefilmde persoon moet derhalve vooraf op de hoogte gebracht worden van elk gebruik en elke verspreiding van de beelden. Hij of zij moet ook worden ingelicht als de beelden buiten de Europese Unie worden doorgegeven.

Bovendien moet de gefilmde persoon toegang hebben tot de beelden die van hem of haar gemaakt zijn en moet hij of zij indien gewenst bezwaar kunnen maken tegen de verspreiding ervan. Er moet ook op gewezen worden dat de persoon die filmt verantwoordelijk is voor de veiligheid van de verwerking. Indien de beelden uitlekken, moet hij of zij de betrokkene daarvan rechtstreeks in kennis stellen.

De European Data Protection Board of EDPB waarin alle gegevensbeschermingsautoriteiten van de lidstaten verenigd zijn, buigt zich momenteel over de problematiek van slimme brillen. Ik wacht dan ook de resultaten van die reflectie af.

01.03 **Kris Verduyckt** (Vooruit): Mijnheer de staatssecretaris, ik ben het met u eens dat het belangrijk is dat mensen hun akkoord moeten geven om gefilmd te worden. In de praktijk blijkt dat echter bijzonder moeilijk te zijn. Iedereen die zo'n bril draagt, moet dan voortdurend aan iedereen die hij tegenkomt vragen of hij mag filmen en beloven om de beelden niet naar het buitenland te versturen.

Het komt op mij over als een producent die een wagen op de markt brengt die minimaal 120 kilometer per uur rijdt.

Ik ben zeer benieuwd hoe die instanties hiernaar kijken. Er wordt toch weer een grens verschoven. Ik heb hier grote vragen bij. Is dit nu een technologie die echt een meerwaarde biedt voor ons sociaal samenzijn? Ik zal net als u dit thema blijven volgen, want ik ben echt benieuwd hoe men erover denkt.

Het incident is gesloten.
L'incident est clos.

02 Vraag van Kris Verduyckt aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen, de Culturele Instel.) over "PimEyes" (55029808C)
02 Question de Kris Verduyckt à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments, des Instit. Culturelles) sur "PimEyes" (55029808C)

02.01 **Kris Verduyckt** (Vooruit): Na de discussies in het Parlement over het platform Clearview, dat ook door de politie gebruikt werd, worden we geconfronteerd met alweer een verdergaande stap, met name met PimEyes. Dat is de eerste openbare website waarop personen kunnen worden teruggevonden op basis van gezichtsherkenning. Als ik een foto zou nemen van de medewerker van de staatssecretaris, weet ik binnen een aantal minuten welke foto's er van de betrokkene op het internet staan. U zou ervan verbaasd staan hoe goed en sterk de website is. Ik zal dat natuurlijk niet doen, want het betreft een illegale toepassing. Allerhande reportages leren ons hoe ver dat gaat.

Ongetwijfeld volgen er nog van dergelijke websites en dat zal ertoe leiden dat niemand straks nog in de openbare ruimte kan komen zonder het risico te lopen dat iemand een foto van hem neemt en zo kan nagaan wie die persoon is. De Duitse datawaakhond, de tegenhanger van de Belgische Gegevensbeschermingsautoriteit (GBA), is ondertussen een onderzoek gestart naar PimEyes. Volgens de Belgische wetgeving mag dat soort websites in principe niet. Op de website wordt wel geargumenteerd dat de toepassing enkel mag worden gebruikt voor de eigen foto's, maar in de praktijk kan dat perfect ook met de foto's van iemand anders.

Hoe kijkt u naar dat soort websites?

Bent u het met mij eens dat die serieuze gevolgen kunnen hebben voor het samenleven?

Is de toepassing gewoon niet illegaal? Gezichtsherkenningssoftware is nu eenmaal verboden in België.

Had u hierover al contact met de GBA?

02.02 Staatssecretaris **Mathieu Michel:** De verwerking van biometrische gegevens is in beginsel verboden op grond van de AVG, met uitzondering van de in artikel 9 van de verordening genoemde uitzonderingen. Als een website gezichtsherkenningssoftware gebruikt zonder de wetgeving inzake gegevensbescherming na te leven, kan hier uiteraard tegen opgetreden worden. Zelfs als een uitzondering mogelijk is, moeten alle andere beginselen van de AVG, zoals het beginsel dat gegevensverwerking evenredig moet zijn, nog steeds in acht worden genomen. In het geval van een inbreuk voorziet de AVG in sancties die financieel of niet-financieel kunnen zijn. Boetes kunnen oplopen tot 20 miljoen euro of 4 % van de totale jaarlijkse wereldwijde

omzet.

In het geval van PimEyes kan ik op basis van de elementen waarover ik beschik, weliswaar voorbehoud maken, maar het is niet aan mij om mij uit te spreken over de onwettigheid van de software. De GBA of een rechter moeten dat doen. De GBA en ik delen op basis van de beschikbare informatie alvast hetzelfde gevoel in verband met het dossier.

02.03 **Kris Verduyckt** (Vooruit): Mijnheer de staatssecretaris, ik ben tevreden over uw erkenning dat dergelijke zaken inderdaad onwettig kunnen zijn. Ik hoop dat de GBA en anderen het publieke debat volgen en dat er opgetreden wordt tegen dergelijke opdringerige websites.

Het incident is gesloten.
L'incident est clos.

03 Vraag van Stefaan Van Hecke aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen, de Culturele Instel.) over "De impact van Bluetooth-trackers op de privacy" (55030439C)
03 Question de Stefaan Van Hecke à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments, des Instit. Culturelles) sur "L'incidence des traceurs Bluetooth sur le respect de la vie privée" (55030439C)

03.01 **Stefaan Van Hecke** (Ecolo-Groen): Mevrouw de voorzitster, mijnheer de staatssecretaris, steeds meer bedrijven verkopen bluetooth-trackers. De apparaatjes zijn bedoeld om een object terug te vinden, zoals sleutels. Ze kunnen echter ook worden misbruikt, om personen te volgen en te stalken, omdat ze klein zijn en eenvoudig te verstoppen.

Sommige bedrijven, zoals Apple, voorzien bij hun AirTags in waarschuwingssystemen die de persoon waarschuwen die wordt gevolgd. Dat werkt echter enkel, indien de persoon zelf een iPhone heeft. Het systeem is ook niet waterdicht.

Het toont echter ook aan hoe bedrijven die innoverende technologie op de markt brengen nog te vaak kunnen opereren buiten een strikt juridisch kader. Daardoor worden problemen genegeerd die reeds kunnen worden voorzien vooraleer het product op de markt wordt gebracht, waardoor de samenleving opdraait voor de negatieve impact op onze privacy en veiligheid.

Daarom heb ik een aantal heel concrete vragen.

Ten eerste, was u reeds op de hoogte van de risico's die dergelijke trackers met zich meebrengen? Indien ja, welke initiatieven hebt u daaromtrent genomen?

Ten tweede, volstaat volgens u onze wetgeving om onze privacy te beschermen? Indien ja, waarom volstaat ze? Indien niet, welke wijzigingen zijn dan eventueel nodig?

Hoe schat u het risico van misbruik in België in? Zal dat risico volgens u de komende jaren groeien door de toenemende populariteit van dergelijke trackers?

Ik kijk uit naar uw antwoorden.

03.02 Staatssecretaris **Mathieu Michel:** Mevrouw de voorzitster, mijnheer Van Hecke, behalve de reeds in uw vraag genoemde kwaadaardige toepassingen zijn er ook cyberveiligheidsrisico's voor de gebruikers van trackers. Die risico's zijn niet specifiek voor de genoemde voorwerpen in het bijzonder, maar betreffen in feite alle geconnecteerde objecten. Het gebruik van een AirTag bijvoorbeeld maakt deel uit van de algemene problematiek van het internet der dingen, dat in de toekomst volledig wettelijk geregeld zal zijn.

In de eerste plaats is er al de AVG, waarin de beginselen van *Privacy by Design and by Default* zijn opgenomen. Die vormde een eerste stap in het rechtskader, maar Europa volgt met andere wetgevende initiatieven, zoals de *Data Act*, die zal bepalen wat mag gebeuren met de data die door die voorwerpen worden verzameld.

Bovendien rijzen er vragen over de verantwoordelijkheid van de maker, de gebruiker, de gebruiksdoeleinden

alsmede bepaalde technische aspecten, zoals de connectiviteit van netwerken.

Zoals met elke nieuwe technologische toepassing die in ons leven komt, verwacht ik dat het risico van misbruik aanvankelijk zal toenemen, maar door waakzaam te zijn en te anticiperen op deze misbruiken zouden we de schade en de schadelijke misbruiken moeten kunnen beperken.

03.03 **Stefaan Van Hecke** (Ecolo-Groen): Mijnheer de staatssecretaris, ik dank u voor het antwoord.

Het incident is gesloten.
L'incident est clos.

04 Samengevoegde vragen van
- Erik Gilissen aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen, de Culturele Instel.) over "Privacy en parkeerapp's" (55030677C)
- Bert Moyaers aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen, de Culturele Instel.) over "Privacylekken in parkeerapps" (55030873C)
04 Questions jointes de
- Erik Gilissen à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments, des Instit. Culturelles) sur "La protection de la vie privée et les applications de parking" (55030677C)
- Bert Moyaers à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments, des Instit. Culturelles) sur "Les fuites de données personnelles liées aux applications dédiées au stationnement" (55030873C)

De **voorzitster**: Van de heer Moyaers hebben we niets vernomen.

04.01 **Erik Gilissen** (VB): Mijnheer de staatssecretaris, het opsporen van mensen via de nummerplaat van hun voertuig blijkt ondertussen erg makkelijk te zijn geworden. De gebruikers van parkeerapps, zoals Indigo en 4411, kunnen via het ingeven van een nummerplaat achterhalen op welke locatie een bepaalde auto geparkeerd staat, dus ook degenen die niet de eigenaar van de auto zijn. Voor mensen met slechte bedoelingen is die kennis natuurlijk heel erg nuttig, want zij kunnen die gebruiken om iemand lastig te vallen, te chanteren of om te achterhalen of iemand thuis is of niet om een inbraak te plannen. Ik heb hierover dan ook enkele vragen.

Bent u van oordeel dat het aangewezen is dat deze informatie wordt afgeschermd en enkel beschikbaar wordt gesteld aan de betrokken actoren en eventueel de veiligheidsdiensten?

Welke maatregelen voorziet u om deze gevoelige informatie af te schermen?

Bij het aanmaken van een professioneel account kunnen er nummerplaten worden opgegeven die niet toebehoren aan de gebruiker of het bedrijf in kwestie. Welke controle acht u hierop mogelijk?

04.02 Staatssecretaris **Mathieu Michel:** Mevrouw de voorzitster, ik zal op de twee ingediende vragen antwoorden.

Mijnheer Gilissen, allereerst wil ik erop wijzen dat zowel locatiegegevens als nummerplaatgegevens persoonsgegevens zijn en dus onder het toepassingsbeleid van de AVG vallen. Dat houdt in dat voor de verwerking van dergelijke gegevens onder meer het bestaan van een wettelijke basis, de inachtneming van het beginsel van minimale gegevensverwerking, de informatie van de betrokkenen en de beveiliging van de persoonsgegevens vereist zijn. Locatiegegevens moeten bovendien met grote zorgvuldigheid worden verwerkt.

Ten eerste, wat het notmyplate.com-initiatief betreft, ik ben in het algemeen geïnteresseerd in elk initiatief dat burgers in staat stelt het gebruik van hun persoonsgegevens beter te controleren en te bewaken of hun bewustwording rond deze kwestie te vergroten.

Aangezien de problematiek die u aanhaalt uiteindelijk slechts een uitvoering van de AVG is, lijkt het mij niet nodig om er een nieuwe verplichting van te maken. De rechten van de gebruikers van websites en apps zijn vastgelegd in de AVG en in de privacywet. Het kader is dus vastgelegd en het is aan de GBA om daarop toe te zien.

Dat brengt mij ertoe erop te wijzen dat de GBA voor de uitoefening van die controleopdracht over verschillende middelen beschikt. Zij kan een onderzoek uitvoeren naar de werking van een informaticasysteem, website of digitale applicatie en kan ook sensibiliseren en gebruikers ondersteunen in het uitoefenen van hun privacyrechten. Zo stelt de GBA op haar website modelbrieven ter beschikking van burgers en bedrijven om hun verschillende rechten in verband met de AVG bij de voor de verwerking verantwoordelijken te doen gelden, meer bepaald het recht van verzet, het recht op overdraagbaarheid en het recht op de beperking van de verwerking.

Daarnaast is niet alleen het privacyluik van belang, maar ook het veiligheidsluik. Het is dus evengoed van belang dat de eigenaars van systemen of toepassingen de kans krijgen om kwetsbaarheden in hun producten aan te pakken voordat deze openbaar worden. Op nationaal niveau fungeert het CCB als anonieme hotline om de ontwikkelaar te informeren over ontdekte kwetsbaarheden. Elke maand worden meer dan 1.000 gerichte waarschuwingen verzonden.

Wat de Europese dimensie van deze problematiek betreft, kan ik u erop wijzen dat de European Data Protection Board of EDPB zich buigt over de bescherming van de privacy van gebruikers van digitale toepassingen. Bovendien zullen de lidstaten krachtens de komende NIS2-richtlijn verplicht zijn een gecoördineerd beleid voor de openbaarmaking van kwetsbaarheden in te voeren en een nationaal cyberagentschap aan te wijzen als nationale coördinator en eventuele neutrale tussenpersoon voor dit doel. In België is dat al het geval.

Ten slotte werkt de EU momenteel aan een cyberweerbaarheidswet. Deze verordening moet ervoor zorgen dat producten met digitale componenten, waaronder toepassingen, zo veilig mogelijk zijn voordat ze op de markt worden gebracht en dat ze gedurende een bepaalde minimumperiode nadat ze op de markt zijn gebracht beveiligingsupdates blijven aanbieden. De tekst werd in september 2022 door de Europese Commissie voorgesteld en de onderhandelingen zullen naar verwachting in 2024 worden afgerond.

04.03 **Erik Gilissen** (VB): Mijnheer de staatssecretaris, dank u voor het antwoord. U verwees naar de GBA voor de controle. Ik stel mij de vraag in hoeverre die daadwerkelijk controles uitvoert. Als men de nummerplaat van iemand anders kan ingeven en zo kan achterhalen waar die zich bevindt, dan is er immers duidelijk een probleem met de privacy.

Het incident is gesloten.
L'incident est clos.

05 Vraag van Kris Verduyckt aan Mathieu Michel (Digitalisering, Administratieve Vereenvoudiging, Privacy en Regie der Gebouwen, de Culturele Instel.) over "Het nieuwe privacybeleid van TikTok" (55031676C)
05 Question de Kris Verduyckt à Mathieu Michel (Digitalisation, Simplification administrative, Protection de la vie privée et Régie des Bâtiments, des Instit. Culturelles) sur "La nouvelle politique de confidentialité de TikTok" (55031676C)

05.01 **Kris Verduyckt** (Vooruit): Mijnheer de staatssecretaris, voortaan laat het privacybeleid van TikTok expliciet toe dat medewerkers uit China en andere landen in de wereld inzage hebben in de data van Europese gebruikers. Dat gaat vrij ver, want zij krijgen nu toegang tot de smartphone van een gebruiker en daarmee ook tot zijn locatiegegevens, camera en microfoon. Experts vrezen dat die data niet alleen bij TikTok blijven, maar uiteindelijk bij de Chinese overheid terechtkomen.

Daarnet hadden we het over het ongeoorloofd gebruik van gegevens, de economische dominantie van internationale spelers en de mogelijke invloed van technologie op het democratische proces. De kwestie die ik hier aankaart, lijkt daarin ook te passen.

Sommige Europese landen zoals Italië hebben al een tijdelijke ban op TikTok ingevoerd. Ik weet niet of men daar in ons land ook aan denkt. Bestaat daar discussie over?

Hoe wordt het gebruik bijvoorbeeld door minderjarigen van dat kanaal gecontroleerd? Op welke wijze wilt u, met de intenties in uw beleidsnota in het achterhoofd, sterker optreden?

05.02 Staatssecretaris **Mathieu Michel:** Er is geen sprake van een ban voor TikTok in België of Europa. Het

gaat er veeleer om dat sociale netwerken onze Europese regelgeving moeten respecteren. Het standpunt van België ter zake is dan ook zeer duidelijk. Zodra persoonsgegevens in Europa worden verzameld, worden de beginselen van de AVG van toepassing, ongeacht de locatie of de nationaliteit van de verantwoordelijke voor de verwerking.

In de AVG staat dat gegevens eerlijk en transparant moeten worden verwerkt en dat de gebruiker van een sociaal netwerk moet worden geïnformeerd over de doeleinden van de verwerking, de ontvangers van de gegevens en de landen waaraan de gegevens worden doorgegeven. TikTok moet zich dus schikken naar die regels. Als dat niet gebeurt, dan kunnen de nationale gegevensbeschermingsautoriteiten op eigen initiatief of op basis van een klacht een onderzoek naar TikTok instellen

Als wordt vastgesteld dat de wetgeving niet wordt nageleefd, dan kunnen de gegevensbeschermingsautoriteiten TikTok verbieden gegevens te verwerken of een boete van maximaal 20 miljoen euro of 4 % van de wereldwijde omzet opleggen. Die controle wordt momenteel ook toegepast. Omdat TikTok het onderwerp van verschillende klachten in Europa is, werd het eenloketsysteem geactiveerd.

De Ierse toezichthoudende autoriteit treedt hierbij op als leidende autoriteit en heeft een onderzoek ingesteld. De GBA wordt via dat mechanisme in kennis gesteld van de door de Ierse autoriteit genomen maatregelen. Mocht de Ierse autoriteit besluiten dat er een inbreuk is van de Europese wetgeving en voorstellen om sancties op te leggen, dan zal zij haar ontwerp van besluit hiertoe voor commentaar aan de GBA en de andere nationale toezichthoudende autoriteiten voorleggen. Aangezien de procedure vertrouwelijk is, kan de GBA momenteel geen verdere informatie verstrekken.

Met betrekking tot de bewustmaking van jongeren is de GBA zeer actief, via de website www.ikbeslis.be, een website voor jongeren, ouders en leerkrachten die gewijd is aan concrete vragen in verband met gegevensbescherming. Er is op de site in het kader van het project bijvoorbeeld een pagina over gegevensverwerking bij het gebruik van mobiele toepassingen.

Voor www.ikbeslis.be heeft de Gegevensbeschermingsautoriteit ook een leespakket ontwikkeld, dat beschikbaar is voor leraren. Tevens stuurt ze regelmatig leesmateriaal naar scholen om jongeren bewuster te maken van gegevensbeschermingskwesties.

05.03 **Kris Verduyckt** (Vooruit): Mijnheer de staatssecretaris, ik dank u voor de informatie over de procedure, www.ikbeslis.be en de verwijzing naar de Europese regelgeving.

Mijn vraag was ingegeven door de uitspraak van eerste minister De Croo, in het kader van een debat in Europa over China onlangs, dat Europa zijn economische relatie met China meer met een strategische bril moet bekijken en naïviteit achterwege moet laten om te vermijden dat China te veel controle krijgt in cruciale sectoren. We moeten de aangehaalde kwestie des te meer van nabij volgen, nu er in de Verenigde Staten steeds meer stemmen opgaan om in te grijpen.

Het is dus goed dat er regelgeving in dat verband bestaat en dat een instelling op de naleving ervan toekijkt, maar we mogen niet naïef zijn. We moeten het medium met bijzondere interesse blijven volgen.

Het incident is gesloten.
L'incident est clos.

De openbare commissievergadering wordt gesloten om 12.37 uur.
La réunion publique de commission est levée à 12 h 37.