



**VAST COMITÉ VAN TOEZICHT
OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN**

Notitienummer : ID/2023/002

Informatiepositie van de inlichtingendiensten met betrekking tot de risico's die inherent zijn aan het gebruik van TikTok

13 april 2023

INHOUDSOPGAVE

1. Inleiding	3
2. Het advies van het CCB en de bijdrage hieraan van de inlichtingendiensten	4
2.1. De informatie van de Veiligheid van de Staat (VSSE)	4
2.2. De informatie van de Algemene Dienst Inlichting en Veiligheid (ADIV)	6
3. Internationaal	9
3.1. Instellingen van de Europese Unie	9
3.2. EU-lidstaten	10
3.3. Verbodsbepalingen elders in de wereld	12
Bijlage 1: Verslag van het Centrum voor Cybersecurity België (CCB)	15
Bijlage 2: Door het Strategisch Comité voor Inlichting en Veiligheid genomen beslissingen, goedgekeurd door de Nationale Veiligheidsraad	16
Bijlage 3: Overzicht per EU-lidstaat van de nationale maatregelen die zijn genomen om de toegang tot de app TikTok te beperken	17
Bijlage 4 : Korte synthese van de technische analyses van Citizen Lab en Check Point over TikTok & Onderzoeken Data Protection Commission (Ierland)	24

1. Inleiding

Op basis van een adviesrapport van het Centrum voor Cybersecurity België (CCB) van 8 maart 2023, opgesteld in samenwerking met de Belgische inlichtingendiensten (zie bijlage 1), besliste de Belgische Nationale Veiligheidsraad (NVR) op 10 maart 2023 om een tijdelijk verbod in te stellen op het gebruik van TikTok op toestellen van de overheidsdiensten omwille van bezorgdheid in verband met privacy en veiligheid.

De door het Strategisch Comité voor Inlichting en Veiligheid genomen beslissingen, die de NVR heeft goedgekeurd¹ zijn als volgt geformuleerd (zie bijlage 2):

1. Voor het personeel van de federale overheid:
 - a. *Verbod, met onmiddellijke ingang, op de installatie en het gebruik van de TikTok applicatie op vaste en mobiele diensttoestellen;*
 - b. *Verwijdering, tegen uiterlijk 31 maart 2023, van alle bestaande TikTok applicaties op deze diensttoestellen;*
 - c. *Aanbeveling om de TikTok applicatie niet te installeren op persoonlijke toestellen met toegang tot interne federale overheidsnetwerken en- systemen, en om deze te verwijderen indien reeds geïnstalleerd;*
 - d. *Het CCB wordt verzocht om na te gaan of de webtoegang tot TikTok geblokkeerd kan worden in de professionele omgeving.*
2. Aan de administraties wordt gevraagd om de toegang tot WiFi-netwerken te differentiëren tussen diensttoestellen en persoonlijke toestellen.
3. De gegevensbeschermingsautoriteit wordt verzocht om een onderzoek op te starten naar het privacybeleid van TikTok.
4. Maximale verspreiding van het advies van het CCB naar de regionale, provinciale en lokale overheden en instellingen.
5. De private sector wordt opgeroepen om waakzaam te zijn voor de potentiële risico's van het gebruik van de TikTok applicatie.
6. Het CCB wordt verzocht om na te gaan of het mandaat van de Nationale Raad voor Cyberveiligheid aangepast of uitgebreid moet worden met het oog op technologische en innovatieve waakzaamheid en hierover een advies te formuleren aan het Strategisch Comité Inlichtingen en Veiligheid.
7. De Eerste Minister en de Minister van Ambtenarenzaken zullen een ontwerprichtlijn voorleggen aan de Ministerraad voor de uitvoering van dit tijdelijk verbod.
8. Het tijdelijk verbod zal geëvalueerde worden na 6 maanden.

Op 17 maart 2023 keurde de federale regering een ontwerp van omzendbrief goed ter uitvoering van de beslissing van de Nationale Veiligheidsraad voor het federale personeel.²

¹ Zie de email dd. 4 april 2023 van de Kabinetschef van de Eerste Minister aan het Vast Comité I.

² Tijdelijk verbod op het gebruik van TikTok voor overheidspersoneel | News.belgium

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

De NVR heeft aan de gewestelijke, provinciale en lokale overheden gevraagd soortgelijke verboden op te leggen en heeft aan de Gegevensbeschermingsautoriteit gevraagd om een onderzoek in te stellen naar het privacybeleid van TikTok.

Vlaanderen had op 9 maart 2023 al een soortgelijke beslissing genomen. Wallonië en het Brussels Hoofdstedelijk Gewest hebben in navolging van de federale regering soortgelijke maatregelen genomen voor het gewestelijk overheidspersoneel. In het Brussels Hoofdstedelijk Gewest geldt het verbod niet voor de persoonlijke toestellen van de ambtenaren, maar wordt niettemin aanbevolen om de applicatie niet te installeren of te gebruiken op persoonlijke toestellen die toegang hebben tot de netwerken van de overheidsadministraties.³ Voor het personeel van het Waals Gewest is een ruimer verbod van toepassing, daar het betrekking heeft op alle toestellen waarop beroepsgerelateerde informatie circuleert evenals op persoonlijke toestellen die toegang hebben tot interne netwerken en systemen.⁴

2. Het advies van het CCB en de bijdrage hieraan van de inlichtingendiensten

Op 28 februari 2023 werd het Centre for Cybersecurity Belgium (CCB) door de Adviseur Cybersecurity van de Beleidscel van de Eerste Minister gevraagd om een advies te verlenen met betrekking tot het gebruik van TikTok door smartphone-gebruikers, behorende tot de overheidsdiensten.

De vraag om advies werd door het CCB doorgestuurd aan de beide Belgische inlichtingendiensten. In concreto vroeg het CCB de diensten om een antwoord op twee vragen: 1/ beschikt u over betrouwbare rapporten of analyses die wijzen op significante veiligheidsrisico's bij het gebruik van de Chinese app TikTok?, 2/ adviseert u dat het gebruik van de Chinese app TikTok op dienstsmartphones van medewerkers van overheidsdiensten wordt verboden?

Het CCB meende dat de tweede vraag van geopolitieke aard was, en dat deze enkel door de inlichtingendiensten kon worden beantwoord.

2.1. DE INFORMATIE VAN DE VEILIGHEID VAN DE STAAT (VSSE)

De VSSE antwoordde op de vragen van het CCB dat de dienst niet over de technische knowhow beschikte om een onderzoek te voeren naar de informatie die circuleert over de veiligheidsrisico's die zijn verbonden aan het gebruik van deze applicatie. De VSSE meent dat met name het Cyber Command van de ADIV beter geplaatst is om in deze advies te verlenen.

De VSSE verwees verder naar zijn antwoorden op parlementaire vragen in het verleden over het onderwerp. De VSSE stelde wel op de hoogte te zijn van een aantal analyses, waaruit blijkt dat de TikTok-app ernstige kwetsbaarheden bevat, en raadde daarom aan om de app niet te installeren op apparaten die voor professionele redenen worden gebruikt, of die gevoelige informatie bevatten.

³ Het Brusselse gewest verbiedt de TikTok-app op de diensttoestellen van zijn personeel | Talent.brussels

⁴ 'TikTok interdit pour le personnel du Gouvernement wallon' (wallonie.be).

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

Het standpunt van de VSSE met betrekking tot het gebruik van de TikTok-app komt tot uiting in het antwoord op een parlementaire vraag waaraan de VSSE een bijdrage leverde. Het betreft een vraag van dhr. Michael Freilich (N-VA) in december 2020.⁵ Dhr. Freilich vroeg of de VSSE reeds een onderzoek voerde naar het gebruik van de TikTok-app, nadat in de Verenigde Staten bezorgdheid was geuit omtrent het verzamelen van persoonsgegevens van Amerikaanse staatsburgers via de app, en nadat ook in Frankrijk en Nederland reeds onderzoeken waren gestart?

De VSSE baseerde zich voor zijn antwoord op open bronnen-informatie die een antwoord tracht te bieden op drie vragen: 1/ vertoont de app kwetsbaarheden op het vlak van veiligheid?, 2/ vormt de app een bedreiging voor de privacy?, 3/ kan de app gebruikt of misbruikt worden voor een bedreiging waarvoor de VSSE bevoegd is?

Wat de mogelijke technische kwetsbaarheden betreft van de TikTok-app, verwees de VSSE naar een aantal technische analyses, onder andere van de gereputeerde cybersecurity onderneming Check Point.⁶ Uit deze analyses blijkt dat hackers het account van een gebruiker volledig kunnen overnemen door het zenden van een gemanipuleerde link⁷, en dat sommige versies van TikTok onveilige http-verbindingen gebruiken om media te downloaden, waardoor hackers privégegevens kunnen stelen of video's kunnen manipuleren.

TikTok is een app waarvan het verdienmodel gebaseerd is op de verwerking van data voor commerciële doeleinden. De ontwikkelaar en beheerder van dit model zal dus trachten een maximaal aantal data over de gebruikers te verzamelen.⁸ Deze data behelzen de inhoud van de communicaties die de gebruikers via de app versturen, maar tevens een aantal metadata zoals de gebruikte hardware, adresboek, locatiegegevens, enz.⁹ Voor het gebruik van de TikTok-app moet de gebruiker een expliciete toestemming geven om toegang te verlenen tot deze informatie. Volgens de VSSE zijn deze toegangsrechten voor het gebruik van de app zeer ruim. De dienst vraagt zich ook af in hoeverre de verzamelde gegevens enkel worden gebruikt voor louter legitieme functionele, en niet voor andere en ongewenste, doeleinden.

Naar een mogelijk misbruik van gegevens van de gebruikers toe in het kader van mogelijke dreigingen waarvoor de VSSE bevoegd is, wijst de dienst op het feit dat TikTok als platform in handen is van het Chinese moederbedrijf ByteDance. Als Chinese onderneming is ByteDance onderworpen aan de compliance regels van de Chinese overheid met betrekking tot de toegang tot gegevens door die Chinese overheid. Hierbij zijn twee specifieke Chinese wetten van belang: de Chinese cybersecurity-wet die netwerkoperatoren verplicht om volledige toegang te verlenen tot hun gegevens aan de Chinese politie- en veiligheidsdiensten, en die deze operatoren ook verplicht tot een niet nader gespecificeerde technische ondersteuning. Ten tweede is er de Chinese

⁵ Vraag van M. Freilich aan de minister van Justitie over 'TikTok' (Vr. en Ant. Kamer 2020-21, 9 december 2020, QRVA 30, 257, Vr. nr. 49).

⁶ <https://research.checkpoint.com/2020/tik-or-tok-is-tiktok-secure-enough/>

⁷ Voor meer informatie over dergelijke technieken, zie Vast Comité van Toezicht op de Inlichtingen- en Veiligheidsdiensten, "Toezichtonderzoek ter navolging van de onthullingen over het gebruik van PEGASUS-software", oktober 2022, p.14-15.

⁸ De beheerder van TikTok in de Europese Unie is TikTok Technology Limited, gevestigd in Dublin, Ierland.

⁹ Het privacybeleid van TikTok, met inbegrip van de rechten van de gebruiker en een oplijsting van de informatie die het bedrijf over de gebruikers verzamelt, kan teruggevonden worden op <https://www.tiktok.com/legal/page/eea/privacy-policy/>

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

inlichtingenwet die alle Chinese organen, burgers en organisaties verplicht om samen te werken met inlichtingen- en veiligheidsdiensten, onder meer door deze toegang te verschaffen tot alle 'relevante' niet-publiek toegankelijke plaatsen.

Het moederbedrijf ByteDance van TikTok heeft volgens de VSSE een verleden van goede samenwerking met de Chinese veiligheidsdiensten. Hoewel TikTok zelf niet beschikbaar is in China, en volgens het bedrijf er geen gegevens worden opgeslagen in China, voorzien de gebruikersvoorwaarden van TikTok wel dat de gegevens mogen worden gedeeld met andere bedrijven die deel uitmaken van dezelfde groep.¹⁰

De VSSE stelt dat zij nog geen concrete gevallen van spionage via de TikTok-app hebben kunnen vaststellen, noch dat in de app expliciete spionagesoftware werd verwerkt. De dienst acht het echter aangewezen om op apparaten voor professionele gebruik, of apparaten waarop gevoelige informatie terug te vinden is, geen apps te installeren die niet noodzakelijk zijn, waaronder de TikTok-app.

In het huidige veiligheidsbeleid van de VSSE, dat in voege trad op 1 maart 2023, is voorzien dat de centrale informaticasectie van de dienst verantwoordelijk is voor de configuratie van de gsm's, smartphones, laptops en ander ICT-materiaal dat aan het personeel voor professionele doeleinden ter beschikking wordt gesteld. Enkel deze sectie bepaalt welke applicaties op deze toestellen geïnstalleerd mogen worden. De installatie van niet-toegestane applicaties wordt geblokkeerd. Ook mag er op deze toestellen geen geclassificeerde informatie worden verwerkt en opgeslagen, en mogen deze toestellen niet worden verbonden met openbare wifi-netwerken.¹¹

2.2. DE INFORMATIE VAN DE ALGEMENE DIENST INLICHTING EN VEILIGHEID (ADIV)

De ADIV deelde aan het Vast Comité I op 27 maart 2023 mee dat de dienst actief heeft deelgenomen aan de discussie in voorbereiding van de beslissing van de Nationale Veiligheidsraad (NVR) om het gebruik van de TikTok-app te verbieden op de officiële diensttoestellen van federale overheidsfunctionarissen. De ADIV adviseerde hierbij zowel de Beleidscel van de minister van Defensie als het CCB, en dit op basis van een analyse die de ADIV reeds uitvoerde in juni 2021. De ADIV benadrukte dat de hernieuwde aandacht voor de gevaren van het gebruik van de TikTok-app niets heeft gewijzigd aan zijn analyse van 2021. De privacy- en veiligheidsrisico's zijn dezelfde gebleven.

De analyse waarnaar de ADIV verwijst werd opgesteld op 2 juni 2021, en dit op vraag van de Gemotoriseerde Brigade van de Landcomponent (Mot Bde-LPB).

Deze analyse bevat een historiek van TikTok en van het Chinese moederbedrijf ByteDance. De dienst wijst erop dat ByteDance in China ook het sociaal mediaplatform Douyin exploiteert, en dat er een aanzienlijk verschil is tussen het privacybeleid van TikTok en Douyin, wat te wijten is aan het feit dat TikTok dit beleid heeft moeten aanpassen aan de wetgeving van de westerse landen waar

¹⁰ ByteDance is actief in meer dan 150 landen, en beheert ook sociale media platforms in China zoals Douyin, Toutiao en Xigua Video. Het bedrijf is ook actief op het vlak van Artificial Intelligence.

¹¹ De VSSE, die op 4 april 2023 werd gecontacteerd om haar definitieve opmerkingen daarover te kunnen maken, heeft (nog) niet gereageerd.

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

het actief is. Hoe dan ook zijn eventuele door TikTok in China opgeslagen gegevens onderhevig aan de Chinese cybersecurity-wetgeving, wat betekent dat de Chinese inlichtingen- en veiligheidsdiensten er toegang toe hebben.

De ADIV wijst ook op het feit dat de oprichter en voormalige CEO Zhang Yiming ontslag nam, eerst als CEO in mei 2021 en later als voorzitter in november 2021, en dat dit mogelijk gebeurde onder politieke druk van de Chinese overheid. Hetzelfde gebeurde in 2021 met andere belangrijke CEO's van Chinese bedrijven, waaronder Alibaba en Pinduoduo. Volgens de ADIV wijst dit er mogelijk op dat de Chinese overheid meer greep wenste te krijgen op multinationale ondernemingen van Chinese oorsprong door de CEO's en voorzitters hiervan te vervangen door meer loyale personen.

De ADIV verwijst naar een aantal technische veiligheidsissues die gepaard gaan met het gebruik van de TikTok-app. De app verzamelt een hele reeks persoonlijke gegevens bij het gebruik ervan: IP-adres, geolocatie, unieke apparaatsidentificators, browsing- en zoekhistoriek, enz. Het gebruikt ook de e-mail login gegevens om de activiteiten van de gebruikers op het platform te volgen. Hierin verschilt TikTok niet van andere sociale mediaplatformen, maar in het geval van TikTok zijn er minder opties beschikbaar voor de gebruiker om zijn/haar privacy-instellingen te beheren. De ADIV maakte specifiek vermelding van een in maart 2021 gepubliceerd rapport van een vergelijkende veiligheids- en privacy-analyse van TikTok en Douyin door Citizen Lab, een gerenommeerd interdisciplinair onderzoekscentrum verbonden aan de University of Toronto.^{12 13}

De ADIV somt in zijn analyse een aantal veiligheidsrisico's op van de TikTok-app, waardoor de gebruikers mogelijk worden blootgesteld aan onder andere phishing en ransomware: het gebrek aan twee-factor identificatie bij het inloggen, het feit dat TikTok gebruik maakt van onversleutelde http-verbindingen ipv. gecrypteerde https om media-inhoud te downloaden via de Content Delivery Networks (CDN), waardoor deze datastromen gemakkelijk kunnen gemonitord en gemanipuleerd worden.¹⁴

Op basis van de geïdentificeerde veiligheidsproblemen die gepaard gaan met het gebruik van de TikTok-app, formuleerde de ADIV in zijn rapport van juni 2021 een aantal aanbevelingen:

- Het sterk ontmoedigen van het gebruik van de TikTok-app.
- Indien de app toch wordt geïnstalleerd, het gebruik ervan beperken op een apparaat dat voor geen enkel ander doeleinde wordt gebruikt, maw. een toestel dat van geen enkele andere app gebruik maakt en geen toegang toelaat tot een netwerk van de Belgische Defensie.
- Enkel informatie verstrekken die absoluut noodzakelijk is voor het gebruik van de app.
- Informatie over locaties enkel beperken tot specifiek toegelaten locaties (geen locaties die in verband kunnen worden gebracht met Defensie).

¹² <https://tspace.library.utoronto.ca/bitstream/1807/123974/1/Report%23137--TikTok.pdf>

¹³ Citizen Lab ontwikkelde in samenwerking met het Security Lab van Amnesty International de Mobile Verification Kit die toeliet om sporen van het gebruik van de spionagesoftware Pegasus te detecteren op smartphones. Vast Comité I, "Toezichtonderzoek ter navolging van de onthullingen over het gebruik van PEGASUS-software", oktober 2022, 30p.

¹⁴ Een CDN is een netwerk van onderling verbonden servers dat het laden van webinhoud voor gegevensintensieve toepassing versnelt door deze inhoud geografisch op servers dichterbij de gebruikers te bewaren.

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

- Het kan wenselijk zijn om gebruikers te verbieden de met de account gepubliceerde video's te downloaden.
- Het is aanbevolen om commentaren op de inhoud te modereren. De app laat toe om commentaren helemaal uit te schakelen, te beperken tot 'vrienden', of ze toe te laten voor iedereen. De app laat toe om via een filter toe te passen op commentaren, en via sleutelwoorden bepaalde commentaren automatisch te verbergen.
- Overwegen om TikTok Business te gebruiken ipv. een persoonlijk account.

Bij deze aanbevelingen benadrukte de ADIV dat het aan de Directie-generaal StratCom toekomt om te beslissen over het al dan niet toelaten van het gebruik van de TikTok-app door de personeelsleden van Defensie.

Het is het Vast Comité I niet bekend in welke mate door de DG StratCom gevolg werd gegeven aan deze aanbevelingen van de ADIV. Wel vermeldt de brief van 27 maart 2023 van de ADIV aan het Vast Comité I dat *"de analyse die de ADIV reeds in 2021 (...) uitvoerde (...) tevens aan de basis lag van het beleid dat het DG StratCom voor Defensie uittekende (...)".*

Het Vast Comité I werd tevens in het bezit gesteld van een door de Chief of Defense (CHOD) uitgevaardigde richtlijn van 20 maart 2023, die uitvoering geeft aan de door de NVR genomen beslissing van 10 maart 2023. Deze richtlijn voert vier te nemen maatregelen in voor het personeel van Defensie: 1/ een verbod, met onmiddellijke ingang, op de installatie en het gebruik van de TikTok-app op de diensttoestellen; 2/ de verwijdering, tegen uiterlijk 31 maart 2023, van de bestaande TikTok-app op deze diensttoestellen; 3/ een verplichting om elk gebruik van TikTok voor officiële communicatiedoeleinden aan DG StratCom te melden; apparaten die voor deze functie zijn bedoeld dienen te worden gebruikt zonder enige andere applicatie of opslag van andere gegevens; 4/ de aanbeveling om de TikTok-applicatie niet te installeren op persoonlijke toestellen met toegang tot interne Defensienetwerken en –systemen en om deze te verwijderen indien reeds geïnstalleerd.

Op 6 april 2023 ontving het Vast Comité I een door de ADIV op 4 april opgesteld, geactualiseerd Cyber Information Report over het gebruik van de TikTok-app.

De ADIV wijst in dit rapport op de vrij recent in China ingevoerde gegevensbeveiligingswet en wet op de bescherming van persoonsgegevens, die de Chinese overheid zou toelaten om bedrijven als TikTok te dwingen om al de door hen verzamelde informatie ter beschikking te stellen van deze overheid.¹⁵ Deze informatie omvat onder andere zoek- en navigatie-informatie, patronen van toestaanslagen, biometrische kenmerken, geolocatiegegevens, metadata, paswoorden, foto- en videobestanden. De direct messaging functionaliteit (chat) ondersteunt geen enkele vorm van end-to-end versleuteling en de app verzamelt niet alleen meta-informatie maar ook de inhoud van de

¹⁵ Analyses van deze wetgeving, die dateren van het derde trimester van 2021, kunnen worden gevonden op onder andere <https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws> en <https://www.lexology.com/library/detail.aspx?g=c7a4a462-7151-4a35-b255-7fe388482f8f>

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

berichten die via de app worden verstuurd. Onversleutelde berichten kunnen worden gelezen door de dienstverlener en door derden, waaronder dus de Chinese overheid.

De samenwerking van TikTok met het cyberbeveiligingsbedrijf HackerOne heeft tal van veiligheidsproblemen en kwetsbaarheden in verband met de app aan het licht gebracht. Het zou gaan om in totaal 582 kwetsbaarheden die door TikTok werden geïdentificeerd en aangepakt. Het rapport van de ADIV somt een aantal van deze kwetsbaarheden op. De dienst wijst er op dat TikTok niet altijd transparant is over de wijze waarop deze veiligheidsproblemen worden opgelost en dat het bedrijf hierover niet altijd de nodige informatie verstrekt in de *changelogs* of *release notes* van de applicatie.

Eén van de kwetsbaarheden van TikTok uit het verleden waarvoor het bedrijf een oplossing heeft ontwikkeld, was de afwezigheid van multi-factor identificatie bij gebruik van de applicatie. Dit werd echter enkel ingevoerd voor de mobiele versie van de app, en niet voor de website. TikTok heeft ook oplossingen ontwikkeld voor verschillende kwetsbaarheden die de diefstal van gegevens van gebruikers toeliet.

Het rapport van de ADIV bevat ook een overzicht van maatregelen die door overheden over de hele wereld werden genomen rond het gebruik van TikTok, en van de reacties hierop van het bedrijf.

Het rapport sluit af met aanbevelingen over het gebruik van de TikTok-app door het personeel van de Belgische Defensie. Deze aanbevelingen zijn strenger dan deze in het rapport van de ADIV van juni 2021 (*zie supra*), en zijn in lijn met de door de CHOD verspreide richtlijn van 20 maart 2023.

3. Internationaal

België is geen uitzondering en verbiedt het gebruik van TikTok door overheidspersoneel. De overgrote meerderheid van de Europese instellingen evenals verscheidene landen binnen en buiten de Europese Unie hebben beperkende maatregelen genomen.

3.1. INSTELLINGEN VAN DE EUROPESE UNIE

Binnen het Europese institutionele landschap besliste de Europese Commissie op 23 februari 2023 als eerste om de installatie en het gebruik van TikTok op de diensttoestellen van haar personeel te verbieden met als doel "*de gegevens van de Commissie te beschermen en de cyberveiligheid te vergroten*".¹⁶ Het verbod van de Commissie geldt ook voor de persoonlijke toestellen waarop beroepsgerelateerde apps worden gebruikt. De Commissie heeft haar personeel gevraagd zo snel mogelijk en ten laatste tegen 15 maart 2023 gevolg te geven aan deze beslissing op straffe van het verlies van de toegang tot de professionele toepassingen (bv. Skype for Business en e-mailaccounts).¹⁷

¹⁶ Volgens de e-mail van de instelling aan haar personeel.

¹⁷ Euroactiv, "*La Commission européenne interdit TikTok sur ses appareils*", 23 februari 2023; Politico, "*Brussels moves to ban Eurocrats from using TikTok*", 23 februari 2023.

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

Verschillende instellingen hebben het voorbeeld van de Commissie gevolgd. Het Europees Parlement deelde op 28 februari 2023 zijn beslissing mee om TikTok te verbieden op de diensttoestellen van het personeel, op grond van bezorgdheid over de veiligheid van de gegevens. De datum van 20 maart 2023 werd vastgesteld als uiterste datum om de app te verwijderen van alle diensttoestellen.¹⁸ Het Parlement heeft zijn medewerkers ook met aandrang aanbevolen om TikTok van hun persoonlijke toestellen te verwijderen.¹⁹

De Raad van de Europese Unie, de Europese Dienst voor extern optreden (EDEO), het Rekenhof, het Europees Comité van de Regio's evenals het Europees Economisch en Sociaal Comité hebben een soortgelijk verbod uitgevaardigd.²⁰

Van zijn kant vond het Hof van Justitie van de Europese Unie het niet nodig een dergelijke maatregel te nemen omdat zijn personeel nooit de mogelijkheid heeft gehad om TikTok te installeren op de diensttoestellen.²¹

3.2. EU-LIDSTATEN ²²

De verschillende EU-lidstaten volgen niet allemaal dezelfde benadering. Terwijl sommige lidstaten een verbod hebben uitgevaardigd of aanbevelingen hebben geformuleerd om het gebruik van TikTok door overheidspersoneel te beperken, hadden heel wat landen eind maart 2023 nog geen beperkende maatregelen uitgevaardigd of althans niet meegedeeld.

(a) Verbodsmaatregelen

In meerdere landen is een verbod opgelegd op de installatie en het gebruik van de TikTok-app op de diensttoestellen van overheidspersoneel, weliswaar met opmerkelijke verschillen wat betreft de draagwijdte van het verbod.

Frankrijk heeft gekozen voor een soortgelijke benadering als in België en kondigde op 24 maart 2023 een verbod aan op de installatie en het gebruik van TikTok op de diensttelefoons van het personeel van alle ministeries. Het verbod in Frankrijk is echter uitgebreider dan in België omdat het niet alleen gericht is op *TikTok* maar op alle zogenaamde "recreatieve" apps. Er is voorlopig nog geen enkele lijst van apps opgesteld, *maar het staat wel vast dat drie grote categorieën van apps in de ban zullen worden geslagen, i.e. spelletjesapps (bv. Candy Crush), apps voor streaming (bv. Netflix) en recreatieve apps (bv. TikTok).*²³

In andere landen zijn er geen gemeenschappelijke algemene richtlijnen voor alle ministeries uitgevaardigd, maar gaat het veeleer om verbodsbepalingen voor het personeel in bepaalde ministeries. Dit is inzonderheid het geval voor de ambtenaren van het ministerie van Defensie en het ministerie van Binnenlandse Zaken in **Duitsland**²⁴, voor het personeel van het ministerie van

¹⁸ Sindsdien zou de internettoegang tot TikTok vanaf de computers van het Europees Parlement zelfs geblokkeerd zijn.

¹⁹ Le Monde, "Après la Commission, le Parlement européen interdit TikTok à son personnel", 1 maart 2023.

²⁰ Euronews, "De plus en plus d'institutions européennes décident d'interdire TikTok sur les appareils de travail", 6 maart 2023.

²¹ *Ibidem.*

²² Bijlage 3 bij deze nota geeft een overzicht van de situatie van land tot land.

²³ Le Monde, "TikTok, Netflix et autres « applications récréatives » interdites sur les téléphones professionnels des fonctionnaires d'Etat français", 24 maart 2023; Franceinfo, "Le gouvernement interdit les "applications récréatives", dont TikTok, Instagram et Twitter, sur les téléphones des fonctionnaires d'Etat", 24 maart 2023.

²⁴ Sinds 2020 voor het personeel van Defensie.

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

Defensie in **Finland**²⁵, in **Denemarken**²⁶ en in **Zweden**²⁷; alsook voor de medewerkers van het ministerie van Buitenlandse Zaken in **Letland**^{28, 29}

Tot slot meldt **Malta** dat het voor overheidspersoneel niet mogelijk is om toegang te hebben tot TikTok of eender welke andere niet-overheidsapp op diensttoestellen.³⁰

(b) Aanbevelingen

Andere lidstaten hebben aanbevelingen geformuleerd om het gebruik van TikTok door overheidspersoneel te beperken. Dit is meer bepaald het geval in **Nederland** waar de regering op basis van een advies van de inlichtingendienst AIVD³¹, besliste, op 21 maart 2023, om haar ambtenaren sterk af te raden om TikTok of andere apps die worden beheerd door landen met een "offensief cyberprogramma" te gebruiken op hun diensttoestellen. Volgens de AIVD bestaat er "een verhoogd risico op spionage" door het gebruik van TikTok of andere apps die worden beheerd door landen met offensieve cyberprogramma's zoals Rusland, China, Iran en Noord-Korea. De Nederlandse regering verklaarde ook nog te zoeken naar een "structurele oplossing" die het onmogelijk maakt deze apps op hun diensttoestellen te installeren.³²

In **Estland** heeft de informatiecontroleautoriteit de overheden aanbevolen om TikTok enkel te gebruiken op toestellen die niet voor beroepsmatig gebruik zijn bestemd. Zonder dat een verbod werd afgekondigd, lieten vijf ministeries weten dat hun personeel TikTok niet gebruikte op diensttoestellen.^{33 34}

In **Slovenië** publiceerde het informatieveiligheidsbureau van de regering op 10 maart 2023 een soortgelijke aanbeveling wegens de risico's op het vlak van cyberveiligheid.³⁵

In **Slowakije** formuleerde het ministerie van Binnenlandse Zaken op 14 maart 2023 voor zijn medewerkers de aanbeveling om TikTok bij wijze van voorzorgsmaatregel niet te installeren of te gebruiken, wegens het bestaan van een ernstige cyberdreiging in verband met de installatie en het

²⁵ Op een onbekende datum.

²⁶ Sinds 5 maart 2023.

²⁷ Sinds 27 maart 2023.

²⁸ Sinds 2 maart 2023.

²⁹ Politico, "Mapped: TikTok faces bans, blocks and probes across Europe", 5 maart 2023; TimeNews, "Swedish Work Mobile Phones Not Allowed to Use Tiktok by the Armed Forces", 27 maart 2023; The Defence Post, "Swedish Military Bans Chinese-Owned TikTok on Work Phones", 28 maart 2023; The Associated Press, "Danish defense ministry bans TikTok on employee work phones", 6 maart 2023; Le Matin, "L'armée interdit à son tour TikTok sur ses appareils", 27 maart 2023; LSM, "Latvian Foreign Ministry bans TikTok on work phones", 2 maart 2023.

³⁰ MaltaToday, "TikTok blocked on government devices just like other social networking sites", 16 maart 2023.

³¹ Algemene Inlichtingen- en Veiligheidsdienst (AIVD), Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, "De Beschouwing risico's gebruik applicaties uit landen met een offensief cyberprogramma gericht tegen Nederland", 23 februari 2023 : Beschouwing risico's gebruik applicaties landen met offensief cyberprogramma gericht tegen Nederland | Brief | Rijksoverheid.nl

³² Nieuwsblad, "Ook Nederlandse regering roept ambtenaren nu op om TikTok te verwijderen van werktelefoon", 21 maart 2023 ; Euroactiv, "TikTok et les applications « à risque d'espionnage » interdites sur les appareils des fonctionnaires néerlandais", 22 maart 2023.

³³ Op 29 maart 2023 liet de minister bevoegd voor informatietechnologie verstaan dat het de bedoeling was een verbod af te kondigen op het gebruik van TikTok op de officiële toestellen van overheidsmedewerkers.

³⁴ Baltic News Network, "Legislative changes needed to completely ban TikTok in Estonia", 3 maart 2023; Eesti Rahvusringhääling (EER), "Complete Tiktok ban in Estonia difficult without amending law", 3 maart 2023; EER, "Minister Järvan: Tiktok to be banned on state officials' work phones", 29 maart 2023.

³⁵ Slovenia Times, "Civil servants urged not to use TikTok", 10 maart 2023.

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

gebruik van de app op de diensttoestellen en de apparaten die toegang hebben tot de informatie- en communicatiesystemen van het ministerie van Binnenlandse Zaken.³⁶

In de **Tsjechische Republiek** vaardigde het Tsjechische nationaal centrum voor cyberveiligheid en informatiebeveiliging (NUKIB) een bindende officiële waarschuwing uit met als doel de toegang tot TikTok te beperken op de zowel professionele als persoonlijke toestellen van personen die onderworpen zijn aan de Tsjechische wet inzake cyberveiligheid.^{37 38}

(c) *Geen maatregelen*

Tot slot hadden meerdere landen, meer bepaald **Luxemburg, Spanje, Portugal, Italië, Oostenrijk, Ierland, Litouwen, Polen, Roemenië**, eind maart 2023 nog geen maatregelen genomen om het gebruik van TikTok door hun ambtenaren te beperken, of hadden ze daarover althans niet gecommuniceerd.³⁹ De meeste landen bleven hun positie evalueren met of zonder lopende technische analyse door hun gegevensbeschermingsautoriteiten.

Sommige staten, zoals Luxemburg en Polen, hebben de Europese Commissie om aanvullende informatie verzocht over de redenen die de aan EU-ambtenaren opgelegde beperkingen rechtvaardigen; voor zover we weten, hebben ze van de Commissie nog geen antwoord gekregen op hun vragen.

3.3. VERBODSBEPALINGEN ELDERS IN DE WERELD

Elders in de wereld hebben verschillende landen en internationale organisaties maatregelen genomen om de TikTok-app te verbieden.

Om te beginnen is het belangrijk om op te merken dat de app in **China** niet toegankelijk is, in tegenstelling tot de Chinese versie ervan, Douyin⁴⁰, die enkel op de Chinese markt beschikbaar is. Hoewel beide apps, TikTok en Douyin, op elkaar gelijken, zijn er toch meerdere verschillen. In antwoord op een verzoek vanwege de Chinese regering om de schermtijd van jongeren te beperken, zorgt de app Douyin ervoor dat de toegang op verschillende manieren wordt beperkt (slechts 40 minuten per dag toegankelijk voor jongeren, pauze van vijf seconden na elke video). Ook de inhoud van Douyin wordt gecensureerd, waardoor bijvoorbeeld inhoud die kritisch is voor de regering of die opkomt voor de rechten van de LGBTQ-gemeenschap wordt verborgen.⁴¹

³⁶ Euroactiv, "Slovak Interior Ministry recommends employees delete TikTok", 15 maart 2023.

³⁷ National Cyber and Information Security Agency - The TikTok app poses a security threat (nukib.cz).

³⁸ Euroactiv, "TikTok représente une menace sécuritaire pour la République tchèque", 9 maart 2023.

³⁹ RTL, "Pour le moment, les fonctionnaires luxembourgeois peuvent utiliser l'appli", 29 maart 2023; Esquire, "¿TikTok podría prohibirse en España?", 17 maart 2023; Expresso, "O TikTok vai ser banido nos EUA? E em Portugal? E haverá realmente perigo? Para quem? 10 perguntas e respostas sobre a polémica", 24 maart 2023; Deutsche Welle, "Italy investigates TikTok over 'dangerous content'", 21 maart 2023; L'avenir, "'Un tournant pour TikTok': le réseau menacé d'interdiction aux USA, déconseillé aux Pays-Bas, sous enquête en Italie", 21 maart 2023; Vienna Times, "Austria Considers Banning TikTok Over Security Concerns", 3 maart 2023; The Storyist, "TikTok ban for Austria's officials? decision before Easter", 24 maart 2023; Irish Mirror, "TikTok could be banned on Irish politicians' phones over security concerns", 23 maart 2023; The Baltic Times, "Lithuanian authorities don't plan to ban TikTok, but advise against using it – official", 28 februari 2023; Euroactiv, "La Pologne va continuer à utiliser TikTok et remet en question l'interdiction de l'UE", 3 maart 2023.

⁴⁰ De app Douyin is eigendom van hetzelfde moederbedrijf, ByteDance.

⁴¹ Le Télégramme, "Interdiction, restriction, enquête... Ces pays qui ont TikTok dans le viseur", 26 maart 2023; BFMTV, "Censure, tradition, interruptions : la version chinoise de TikTok est bien différente de la nôtre", 3 maart 2023.

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

In **India** geldt sinds eind juni 2020 een volledig verbod op de app. Vóór de blokkering van de app was TikTok er razend populair, met meer dan 200 miljoen gebruikers. Deze beslissing, volgens officiële bronnen ingegeven door redenen van nationale veiligheid, werd genomen na een dodelijk conflict tussen India en China langs hun beider grens in de regio Ladakh die ze met elkaar betwisten. Het verbod heeft betrekking op ca. 200 Chinese apps.⁴²

In de **Verenigde Staten** werd de bezorgdheid over TikTok al door voormalig president Donald Trump aangekaart op nationaal niveau.⁴³ In december 2022 verbood het Amerikaanse Congres de toegang tot TikTok op de toestellen en netwerken van de federale regering.⁴⁴ Op 27 februari 2023 liet het Witte Huis aan de federale agentschappen weten dat ze krachtens deze wetgeving 30 dagen de tijd kregen om de app te verwijderen van alle overheidstoestellen. De federale wetgever overweegt nog verder te gaan. Op 1 maart 2023 stemde een commissie van het Huis van Afgevaardigden voor wetgeving waarmee aan president Biden de bevoegdheid wordt verleend om TikTok te verbieden op alle apparaten in het hele land. Op 23 maart 2023 werd Shou Chew, CEO van TikTok, ondervraagd over de banden die de app onderhoudt met het moederbedrijf en over de mogelijke invloed van China op het platform; dit gebeurde tijdens een ongeveer vijf uur durende getuigenis voor de commissie voor Energie en Handel van het Huis van Afgevaardigden.⁴⁵

In **Canada** is de app sinds eind februari 2023 verboden op de mobiele toestellen die de regering ter beschikking stelt van haar personeel, wegens "*een onaanvaardbaar risiconiveau*" voor de persoonlijke levenssfeer en de veiligheid.⁴⁶

Sinds 16 maart 2023 wordt TikTok ook verboden bij wijze van "voorzorgsmaatregel" en "uit vrees voor de veiligheid" op regeringsapparaten in het **Verenigd Koninkrijk**.⁴⁷

In **Noorwegen**⁴⁸, mogen Noorse ministers, staatssecretarissen en politieke adviseurs TikTok of Telegram sinds halverwege de maand maart 2023 niet meer gebruiken op hun officiële toestellen. Het Noorse parlement volgde het voorbeeld van de regering door een soortgelijk verbod voor zijn leden af te kondigen.⁴⁹

Ook **Taiwan** verbiedt sinds december 2022 het gebruik van TikTok op de communicatieapparatuur van de overheid.⁵⁰

⁴² Courrier International, "*Leçons. Trois ans après avoir interdit TikTok, l'Inde est passée à d'autres applis*", 4 maart 2023; The New York Times, "*Why Countries Are Trying to Ban TikTok*", 27 maart 2023.

⁴³ Trumps administratie had verschillende decreten aangenomen, die in de rechtbank werden aangevochten, om TikTok te verbieden. President Biden had in 2021 de maatregelen van zijn voorganger vernietigd en opgeroepen tot een onderzoek om te bepalen welke risico's de app meebrengt alvorens de strijd van zijn voorganger voort te zetten.

⁴⁴ Heel wat Amerikaanse staten hebben soortgelijke maatregelen genomen of overwogen om dat te doen. Op te merken valt dat de toepassing reeds drie jaar verboden was op de overheidstoestellen die door Defensie worden gebruikt.

⁴⁵ The New York Times, "*Why Countries Are Trying to Ban TikTok*", 27 maart 2023; BBC News, "*3 raisons pour lesquelles TikTok pourrait être interdit aux États-Unis*", 29 maart 2023; CBS News, "*Why TikTok faces bans in the U.S.*", 2 april 2023; Euroactiv, "*La Maison Blanche ordonne aux agences fédérales de bannir TikTok de leurs appareils sous 30 jours*", 28 februari 2023; Courrier International, "*Tensions avec la Chine. TikTok risque-t-il d'être banni des États-Unis ?*", 4 februari 2023.

⁴⁶ Le Télégramme, "*Interdiction, restriction, enquête... Ces pays qui ont TikTok dans le viseur*", 26 maart 2023.

⁴⁷ Le Monde, "*Le Royaume-Uni interdit TikTok sur les appareils gouvernementaux*", 16 maart 2023.

⁴⁸ De Overeenkomst betreffende de Europese Economische Ruimte is de meest verstrekkende economische overeenkomst die Noorwegen tot vandaag toe heeft gesloten en vormt de hoeksteen van de betrekkingen tussen Noorwegen en de Europese Unie.

⁴⁹ Scienenorway, "*Top politicians are not allowed to have TikTok on their phones. But why ?*", 27 maart 2023.

⁵⁰ Taiwan News, "*Taiwan bans TikTok from public sector devices*", 6 december 2022.

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

In **Nieuw-Zeeland** besliste het parlement dat de app vanaf 31 maart 2023 niet langer toegankelijk zou zijn op de toestellen van de parlementsleden en meer in het algemeen van zij die toegang hebben tot het netwerk van het parlement.⁵¹

In **Australië** besliste de minister van Justitie op 4 april, op basis van het advies van de inlichtingen- en veiligheidsdiensten, om het gebruik van TikTok te verbieden op alle toestellen die door alle regeringen en agentschappen van de Commonwealth ter beschikking worden gesteld.

In andere landen, zoals **Bangladesh, Pakistan, Indonesië, Afghanistan** en **Iran**, werd de toegang tot TikTok eveneens meermaals, al dan niet tijdelijk, verboden.⁵²

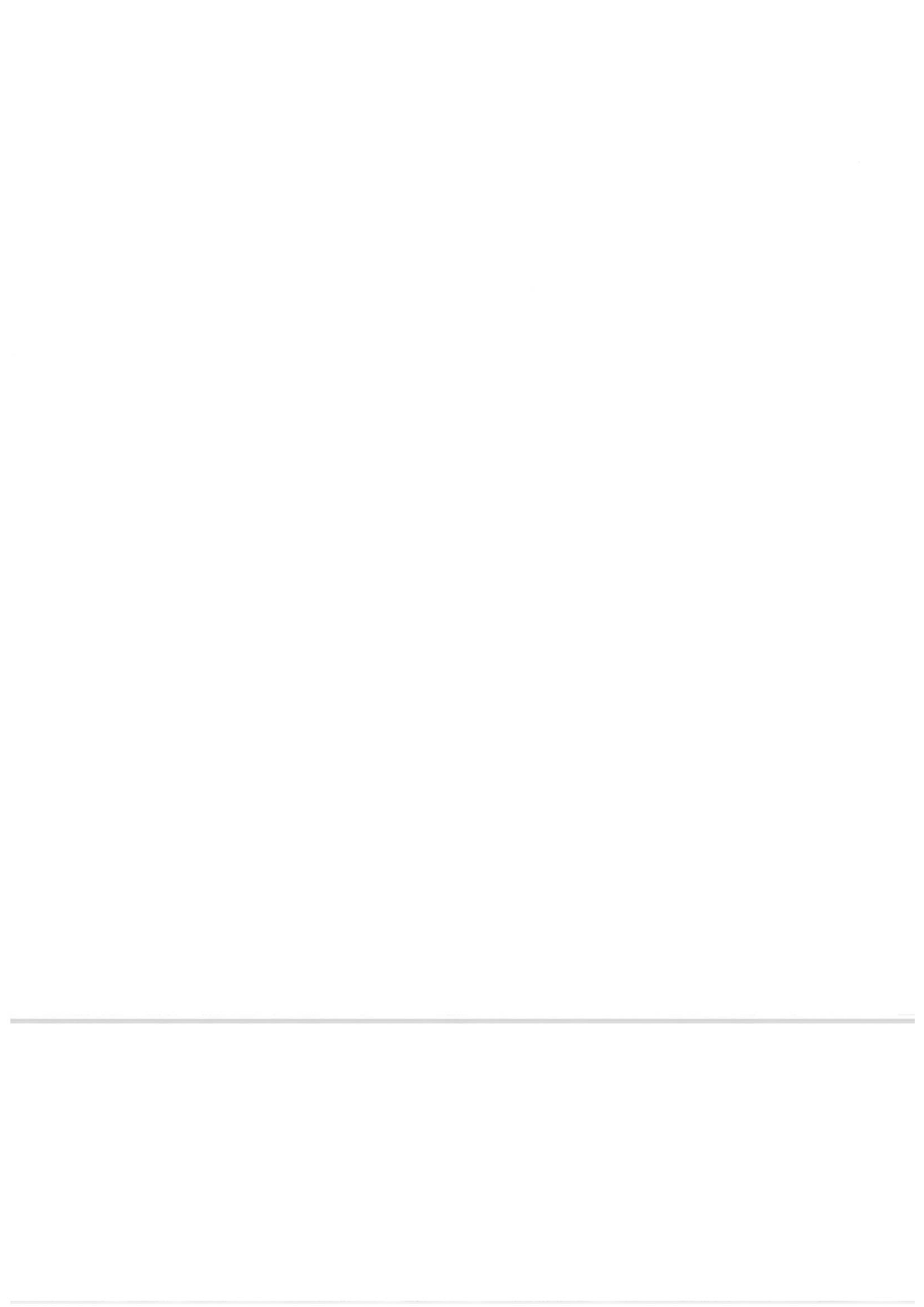
Sinds 31 maart 2023 verbiedt de **NAVO** haar personeel om veiligheidsredenen om de app TikTok nog te downloaden op de toestellen die deze organisatie ter beschikking stelt. In werkelijkheid was TikTok eerder al niet beschikbaar op door de NAVO geleverde toestellen als gevolg van interne technische beperkingen.⁵³

⁵¹ Le Monde, "En Nouvelle-Zélande, TikTok interdit à la Chambre des représentants", 17 maart 2023.

⁵² Le Télégramme, "Interdiction, restriction, enquête... Ces pays qui ont TikTok dans le viseur", 26 maart 2023; Business Insider, "Here's every country that has partially or completely banned TikTok as the US threatens a nationwide ban", 24 maart 2023.

⁵³ CNN, "NATO bans TikTok on devices", 31 maart 2023.

Bijlage 1: Verslag van het Centrum voor Cybersecurity België (CCB)





CENTRE FOR
CYBER SECURITY
BELGIUM

Adviesrapport TikTok

(8 maart 2023)

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 18 – Brussels

T. : +32 2 501 05 63



UNDER THE AUTHORITY
OF THE PRIME MINISTER

.be

Inhoudstabel

<i>Context</i>	3
<i>De uitdaging volgens open source bronnen</i>	3
<i>Internationale reactie</i>	4
<i>VS</i>	4
<i>Europa</i>	5
<i>Elders in de wereld</i>	6
<i>Input VSSE</i>	7
<i>Advies ADIV</i>	9
<i>Technische analyse van het CCB</i>	10
<i>Conclusie en advies</i>	12

Context

TikTok is een dienst die korte video's host, video's die via de TikTok smartphone applicatie kunnen gemaakt, bewerkt en ingestuurd worden, en vervolgens door andere gebruikers kunnen worden bekeken. Gebruikers krijgen in de smartphone applicatie deze video's aangeboden op basis van hun voorbije individuele activiteit op de app. Binnen de app kan doorgelikt worden naar inhoud die aangeboden wordt in een browser binnen de app.

De dienst werd in september 2016 in China op de markt gebracht onder de naam Douyin, en werd vanaf september 2017 als een aparte dienst en applicatie aangeboden op de internationale markt, in meer dan 75 talen. Volgens het analyse bedrijf Sensor Tower was de app in het eerste jaar al 104 miljoen keer geïnstalleerd en eind februari 2023 wereldwijd al 3,5 miljard keer gedownload.

De dienst is eigendom van het Chinese internettechnologiebedrijf ByteDance, dat hoofdvestiging heeft in Beijing.

De uitdaging volgens open source bronnen

Gegeven de grote populariteit van de applicatie en het feit dat het aangeboden wordt door een bedrijf uit China, maakt dat TikTok vrij snel de aandacht trok van regulerende overheden, privacy voorstanders en nationale veiligheid experts.

De bezorgdheden rond de app raken onder andere aan 3 gerelateerde maar verschillende aspecten: vergaring van data, delen met de overheid, en beïnvloeding.¹

In open bronnen worden vermoedens geuit dat TikTok **data zou verzamelen van de gebruikers**, waaronder hun locatie, hun type smartphone, hun gedrag binnen de app en op websites die via de app bereikt worden in de TikTok browser, wat zou kunnen leiden tot het buit maken van creditcard nummers en wachtwoorden.² Deze data verzameling zou volgens sommige onderzoekers gebeuren in grote hoeveelheden en zonder de expliciete toestemming van de gebruikers, wat in tegenspraak is met de Algemene Gegevensbeschermingsverordening (GDPR). Er is ook een specifieke bezorgdheid naar de privacy van minderjarigen, die een heel grote groep uitmaken van de gebruikers. TikTok zelf

¹ https://www.bbc.com/news/technology-64797355?at_medium=RSS&at_campaign=KARANGA

² <https://www.cnet.com/tech/services-and-software/TikToks-in-app-browser-can-monitor-your-keystrokes-researcher-says/>; <https://krausefx.com/blog/announcing-inappbrowsercom-see-what-javascript-commands-get-executed-in-an-in-app-browser>

ontkent alle aantijgingen en volgens andere onderzoekers zou TikTok niets van dit alles doen in een mate die erg verschilt dan andere gelijkaardige sociale media platformen. Sommige gegevensbeschermingsautoriteiten hebben echter reeds boetes opgelegd aan TikTok voor onduidelijk beleid in het behandelen van persoonlijke data (zie punt Internationale reactie hieronder).

Internationale analisten wijzen er op de **Chinese Nationale Inlichtingenwet** van 2017 bepaalt dat alle Chinese organisaties en burgers legaal verplicht zijn om steun, bijstand en medewerking te verlenen aan de Chinese inlichtingendiensten. Sommige media hebben ook gerapporteerd dat sommige medewerkers van de app weldegelijk toegang zouden gehad hebben tot data van gebruikers. TikTok reageerde dat het om individuele gevallen gaat, en sommige onderzoekers nuanceren de legale slagkracht van de vermelde verplichtingen van de Inlichtingenwet als het aankomt op dergelijke datadeling. TikTok/ByteDance zelf beweren immer dat ze dergelijke datadeling nog nooit gedaan hebben noch kunnen of zullen doen, en dat data bovendien niet in China opgeslagen zou worden.

TikTok is een van de weinige populaire sociale mediaplatformen die niet door Amerikaanse bedrijven wordt aangeboden. De grote populariteit van de app leidt zo tot bezorgdheden over spionage, o.a. en erg specifiek van overheidspersoneel dat de app zou gebruiken.

Tot slot is er volgens publieke bronnen de bezorgdheid dat TikTok, en bij extensie de Chinese overheid, **het algoritme zou kunnen controleren** dat bepaalt welke inhoud gebruikers te zien of net niet te zien krijgen in de app. Onderzoekers zijn verdeeld of dergelijke censuur en beïnvloeding effectief gebruikt wordt in TikTok maar de theoretische mogelijkheid zou aanwezig zijn, zoals in vele sociale media platformen.

Daarnaast blijft er de algemene bezorgdheid welk effect TikTok als een sociale media platform kan hebben op het gedrag (en aankoopgedrag) van gebruikers. Minderjarigen – een kwetsbare en grote groep van gebruikers – zijn hierin een groot aandachtspunt. Het platform kan uiteraard, net als andere sociale media, ook gebruikt worden voor propaganda doeleinden van andere actoren, zoals van Rusland. Via het algoritme dat zich baseert op de interesses van gebruikers, zouden bezoekers van de app steeds meer gevangen kunnen worden in een enkel narratief, zonder andere alternatieven.

Al deze bezorgdheden worden voornamelijk versterkt door de toenemende geopolitieke spanningen tussen de VS en China, en dit op vele domeinen.

Internationale reactie

VS

Niet verrassend kwam de meest vocale reactie op de mogelijke dreigingen rond TikTok tot nog toe uit de Verenigde Staten. Onderzoekers wezen het platform aan als een bedreiging voor de nationale

veiligheid voor het land, in een gelijkaardige lijn als Huawei.³ Verschillende politieke vertegenwoordigers vroegen onderzoeken, en in augustus 2020 nam President Trump stappen om een algemene ban op TikTok in te voeren indien het platform niet verkocht zou worden. Het verbod werd tegengehouden door de rechtbanken.

De nieuwe regering van President Biden trok in juni 2021 de eis van President Trump in maar startte een onderzoek naar de nationale veiligheidsrisico's van de app.

In juni 2022 riep de Commissaris van de FCC Apple en Google op om TikTok niet meer aan te bieden op hun appstores, uit bezorgdheid voor de dataverzameling van de dienst bij burgers.

Recent vaardigde President Biden een besluit uit dat binnen de 30 dagen TikTok moet verwijderd zijn van alle overheidsapparaten in de Federale overheid. Ook verschillende Amerikaanse staten vaardigden eerder al gelijkaardige besluiten uit.

Europa

Europa is pas in de laatste maanden meer uitgesproken over haar houding ten opzichte van de mogelijke gevaren van de app. In eerste instantie betrof het boetes opgelegd aan TikTok voor onvoldoende privacybeleid. Daarnaast ligt de focus momenteel, in navolging van de VS, op het verbieden van de app op apparaten van overheidsdiensten.⁴

Reeds in juli 2021 legde de Nederlandse gegevensbeschermingsautoriteit (GBA) TikTok een boete op van €750.000 voor het schenden van de privacy van minderjarigen. De overheid maakte een aanbeveling dat de app best vermeden werd tot het databeschermingsbeleid van de app zou aangepast worden. De Ierse GBA finaliseert momenteel nog een onderzoek naar dezelfde praktijken. In december 2022 legde de Franse GBA (CNIL) TikTok eveneens een boete op, van €5 miljoen, omdat gebruikers van tiktok.com cookies niet even makkelijk konden weigeren en omdat gebruikers niet voldoende geïnformeerd werden over het gebruik van de cookies.⁵

Enkele lidstaten en Europese instellingen hebben een echt verbod ingesteld op de app.

³ <https://www.piie.com/blogs/china-economic-watch/growing-popularity-chinese-social-media-outside-china-poses-new-risks>

⁴ <https://pro.politico.eu/news/160380>

⁵ <https://www.cnil.fr/en/cookies-cnil-fines-tiktok-5-million-euros>

- **Finland** gebood reeds in augustus 2022 overheidsmedewerkers om de app te verwijderen van werk apparaten.
- **Estland** verbood eveneens dat medewerkers van het ministerie van defensie de app zouden installeren, niet enkel op professionele maar **ook op persoonlijke apparaten**.
- Eind februari 2023 verbood de **Europese Commissie**, snel gevolgd door de **Europese Dienst voor Extern Optreden**, het **Europese Parlement** en **Raad van de EU**, dat hun medewerkers de app gebruiken op apparaten gelieerd aan werkgebruik.⁶

Andere lidstaten zijn minder strikt:

- In **Denemarken** adviseren de voorzitter van het parlement en het nationale cybersecurity centrum sterk dat hun medewerkers de app verwijderen van hun telefoons, minstens die voor professioneel gebruik.
- In **Duitsland** is er geen algemeen beleid, en het valt aan elke overheidsdienst apart om een beslissing te nemen over het gebruik van de app. Het Duitse ministerie van defensie heeft al sinds 2020 het gebruik van de app gelimiteerd. Ook in het ministerie van binnenlandse zaken kan de app niet bereikt worden en de installatie ervan op officiële werktelefoons is technisch onmogelijk gemaakt. Het Duitse Cybersecurity agentschap BSI vaardigde adviezen uit.

De meeste lidstaten, zoals **Letland, Spanje, Ierland, Polen, Frankrijk, Italië en Nederland** evalueren echter nog hun positie, en monitoren de evoluties op nationaal en Europees niveau, al dan niet met lopende technische onderzoeken van de gegevensbeschermingsautoriteiten naar het beleid van TikTok.

In Frankrijk heeft de Senaat zich reeds bereid getoond een eigen onderzoek te voeren naar het misbruik van data en beïnvloedingsstrategieën door TikTok. Ook de Franse President Macron sprak zich uit over de gevaren van de app.

In Italië sprak Matteo Salvini zich uit tegen het verbod dat door de Europese Commissie werd uitgevaardigd.

Elders in de wereld

Op dit moment zou TikTok naar verluidt in het algemeen verbannen zijn (niet enkel voor overheidsdiensten) in verschillende Aziatische landen, waaronder Afghanistan, Armenië, Azerbaidjan,

⁶ <https://pro.politico.eu/news/160219>

Bangladesh, India, Iran, Pakistan en Syrië. De app zou eerder reeds tijdelijk gebannen zijn in Indonesia en Jordanië, maar deze ban zou sindsdien in beide landen terug opgeheven zijn.

Op 27 februari kondigde **Canada** aan dat het met onmiddellijke ingang het gebruik van TikTok op apparaten van de federale overheid verbiedt, daar de app een onaanvaardbaar risico bevat ten opzichte van privacy en veiligheid. Hoewel er geen bewijs was dat de app reeds overheidsinformatie zou bemachtigd hebben, oordeelde de overheid dat het risico dat dit zou gebeuren te groot was om toe te laten. De databeschermingsautoriteit in Canada start eveneens een onderzoek, met een focus op het behandelen van persoonlijke data van minderjarigen.

Het **Verenigd Koninkrijk** is voorlopig nog verdeeld over het onderwerp. Het parlement sloot haar eigen TikTok account af in augustus 2022 en sommige overheidsdiensten gebruiken de app niet meer. De minister voor technologie, Donelan, sprak zich echter uit tegen een algemeen verbod voor het gebruik van TikTok door overheidspersoneel. Dit moet een persoonlijke keuze blijven.⁷

Input VSSE

Hierbij volgt een relevant extract van de verschillende antwoorden van de VSSE.

VSSE rond TikTok:

1) Security-experts hebben in het verleden ernstige kwetsbaarheden in de Tiktok app ontdekt. Een voorbeeld hiervan werd aan het licht gebracht door onderzoekers van het gereputeerde cybersecurity onderzoeksbureau Checkpoint.

...

2) TikTok is een 'free-to-use' social media platform. Kenmerkend hierbij is dat het verdienmodel vaak gebaseerd is op het verzamelen en verwerken van data voor commerciële doeleinden. Deze data bestaat enerzijds uit informatie over de inhoud die gebruikers versturen via het platform. Anderzijds is er alle metadata rond het gebruik van de applicatie. Deze kan allerlei vormen aannemen, zoals informatie over het toestel en gebruikte verbindingen, het adresboek van de gebruiker, tot het tijdstip en locatiegegevens. De gebruiker dient toestemming te geven om dit soort informatie te delen, maar dit is vaak een essentiële voorwaarde om de app te kunnen gebruiken. In de praktijk is er dus niet echt sprake van een geïnformeerde keuze voor de gebruiker, of een optie om zijn privacy beter te beschermen. Wanneer we kijken naar de toegangsrechten die gevraagd worden door de TikTok applicatie, kunnen we vaststellen dat deze heel breed gaan.

⁷ <https://www.politico.eu/article/tech-minister-tiktok-should-be-personal-choice-for-uk-officials/>

...

3) TikTok is als social media platform in handen van het Chinese bedrijf ByteDance. Dit bedrijf is dus onderworpen aan de Chinese compliance regels met betrekking tot de toegang van de Chinese overheid tot de data verzameld door ByteDance. Dit bedrijf heeft een track record van goede samenwerking met de Chinese overheid, zie bijvoorbeeld het opdoeken in China van Neihan Duhanzi (een social media platform in China waarop grappen werden gedeeld). TikTok is niet beschikbaar in China en de data worden volgens ByteDance ook niet opgeslagen in China. Maar in de gebruiksvoorwaarden van TikTok wordt wel degelijk vermeld dat de data gedeeld mogen worden binnen de groep. Bovendien hebben experts (Penetrum) vastgesteld dat meer dan 30% van de verbindingen die TikTok maakt naar IP adressen in China gaan. Volgens dezelfde experts worden de TikTok data opgeslagen op servers van de Chinese internetprovider Alibaba die goede banden heeft met de Chinese overheid, en zou TikTok zich bezondigen aan verregaande tracking van gebruikers. Kortom, die gebruikers mogen niet dezelfde bescherming van hun privé-gegevens verwachten als wat ze gewoon zijn binnen de EU.

Hierbij willen de aandacht te vestigen op twee Chinese wetten die van toepassing zijn op ByteDance en dus ook de gegevens die via TikTok verzameld worden.

Ten eerste is er de Chinese cybersecurity wet die netwerkoperatoren verplicht om samen te werken met Chinese politie- en veiligheidsdiensten. Op vraag van de veiligheidsdiensten dienen deze bedrijven volledige toegang te geven tot hun data. Er is ook een verplichting tot een niet nader gespecificeerde 'technische ondersteuning'.

Ten tweede is er de 'intelligence law' die de relatie tussen de veiligheidsdiensten en de Chinese maatschappij regelt. Deze verplicht organen, organisaties en burgers om de nodige ondersteuning, assistentie en samenwerking te voorzien aan de veiligheidsdiensten. Ze geeft deze diensten ook het recht om zichzelf toegang te verschaffen tot alle 'relevante' niet-publieke plaatsen en bronnen. En daar informatie te verzamelen. Wat is hierbij relevant? Onder andere het publiceren of verspreiden van boodschappen die de staatsveiligheid in gevaar brengen en van gefabriceerde of gemanipuleerde feiten. Begrippen die heel breed geïnterpreteerd kunnen worden door een regime met een bijzondere invulling van principes zoals mensenrechten, privacy, vrije meningsuiting of de scheiding tussen recht en staat.

...

Met betrekking tot Chinese smartphones vermeldt de VSSE het volgende:

Ondanks het gebrek aan waargenomen bewijs dat de toestellen worden ingezet voor spionagedoeleinden, kunnen we – uit informatie beschikbaar via open bronnen (i.c. de Chinese wetgeving waarin de producenten opereren) - afleiden dat de theoretische mogelijkheid bestaat dat

de apparaten en de informatie die ze verwerken blootgesteld worden aan Chinese spionage. We adviseren dan ook om waakzaam te zijn, in het bijzonder wanneer het om gevoelige data gaat.

...

Er bestaat vermenging tussen de genoemde bedrijven en de Chinese overheid.

Deze vermenging uit zich op een aantal manieren.

- (1) Ten eerste onderhoudt de Chinese Communistische Partij (CCP) een stevige ideologische grip op de Chinese bedrijven. Deze privébedrijven dienen zich te houden aan de rode lijnen die de CCP uitzet, anders zien zij zich verstoken van toegang tot financiering of worden zij op andere manieren tegengewerkt. Bovendien hebben bedrijven van het formaat van Huawei, Xiaomi, Oppo en OnePlus een partijcomité van de CCP binnen het bedrijf. De taak van dergelijke partijcellen binnen bedrijven is ervoor zorgen dat de beleidslijnen van de CCP ook door het bedrijf worden gevolgd. Partijcellen kunnen invloed uitoefenen op de beleidsbeslissingen van (privé)bedrijven.*
- (2) De vermenging met de Chinese overheid en haar inlichtingen- en veiligheidsdiensten wordt ook juridisch vastgemetseld. Bij wijze van illustratie wensen wij uw aandacht te vestigen op Artikel 7 van de Chinese nationale inlichtingenwet die alle Chinese bedrijven verplicht tot samenwerking met de inlichtingendiensten. Artikel 24 vereist van bedrijven om arbeidsposities te reserveren voor inlichtingenpersoneel. De Chinese cybersecurity wetgeving uit 2016, aangevuld in 2018, verplicht Chinese bedrijven overigens een ongebreidelde toegang tot de IT systemen te verlenen aan de inlichtingendiensten. Samenvattend kunnen we dus stellen dat het bedrijfsleven geen andere keuze heeft dan samen te werken met de Chinese overheid. Er is dus sprake van een systematische en diepgaande vermenging.*

...

Daarom is het aan te raden om op apparaten voor professioneel gebruik, of waarop gevoelige informatie staat, geen apps te installeren die niet noodzakelijk zijn. Dit advies is zeker van toepassing op Chinese apps zoals TikTok.

Opmerking bij de input van VSSE

De VSSE geeft aan geen gericht of diepgaand onderzoek te hebben uitgevoerd naar de producten van Chinese bedrijven zoals ByteDance (TikTok), Huawei, Xiaomi, Oppo, OnePlus, etc, maar dit is volgens het CCB ook niet nodig en ondergeschikt aan de conclusies en het informatie van de VSSE mbt de geopolitieke dreiging.

Advies ADIV

ADIV heeft intern Defensie het gebruik van TikTok sterk afgeraden wegens problemen voor zowel privacy als security. Het gebruik voor dienstredenen moet aangevraagd worden, zo niet is het verboden.

Binnen Defensie is er geen individueel verbod, wel ontrading en een verbod voor officieel gebruik door eenheden.

Technische analyse van het CCB

Het is een **complex dossier met heel wat aspecten en verschillende invalshoeken**. Het is niet duidelijk tot welke informatie TikTok allemaal toegang heeft, maar het is eigen aan sociale media App's om heel veel persoonlijke gegevens, locatie, contacten, website bezoek, etc te verzamelen. TikTok moet zich bij het verzamelen en verwerken van persoonlijke data houden aan de Europese regels van de GDPR. Het is aan de Belgische en andere Europese Gegevensbeschermingsautoriteiten om te analyseren of TikTok voldoet aan deze vereisten.

Er zijn enkele Europese wetgevingen die goedgekeurd of voorgesteld zijn die eveneens kunnen bijdragen. Er is reeds de Algemene Gegevensbeschermingsverordening, waar TikTok dient aan te voldoen, en verschillende autoriteiten hebben reeds onderzoeken en boetes uitgevaardigd in dit kader.

Vanaf midden 2023 komt ook de **Digital Services Act**⁸ in voegen, die nieuwe regels oplegt aan digitale operatoren rond content moderation. TikTok zal zich aan deze regels dienen te houden, wat een antwoord kan bieden aan enkele van de bezorgdheden rond beïnvloeding en ongeoorloofde inhoud.

Ook de in 2022 goedgekeurde **Digital Markets Act**⁹, die regels rond competitie van online platformen vastlegt, zou van toepassing kunnen worden op TikTok.

De Cyber Resilience Act werd voorgesteld in september 2022, en wil veiligheidsvereisten opleggen aan alle producten met digitale elementen, waaronder mobiele applicaties. Wanneer deze verordening goedgekeurd en geïmplementeerd wordt (niet in de eerst komende 2 jaar) zal TikTok ook aan deze cyberveiligheidsvereisten moeten voldoen, wat een verhoging van de veiligheid zou kunnen inhouden.

⁸ https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

⁹ https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

Het belangrijkste voor deze analyse is echter het **cybersecurity aspect**.

Vormt het gebruik van de TikTok software op systemen van overheidsdiensten een veiligheidsrisico?

Het CCB beschikt momenteel **niet over technische rapporten of analyses om TikTok als fundamenteel onveiliger aan te wijzen dan andere gelijkaardige apps.**

Het ontbreken van dergelijke technische rapporten of analyses is echter meestal triviaal. Het risico zit niet in het product maar in de toegang tot informatie die de producent krijgt. De producent heeft dus geen technische kwetsbaarheden of backdoors nodig om informatie te verzamelen.

Met smartphone App's moet er van worden uitgegaan dat de producent sowieso permanent toegang heeft tot heel wat persoonlijke informatie van de gebruiker. De meeste gebruikers van een smartphone geven a priori alle gevraagde toegang bij de installatie van een nieuwe App. **Bovendien vermeldt de VSSE dat heel wat verbindingen van de TikTok app gemaakt worden met IP adressen in China, dat de data wordt opgeslagen op servers van de Chinese internetprovider Alibaba die goede banden heeft met de Chinese overheid en dat Tiktok zich zou bezondigen aan verregaande tracking van gebruikers.**

De technische bezorgdheden rond ongeoorloofd datadeling door TikTok waar in de media naar wordt gerefereerd zijn daarom **voornamelijk risico's van geopolitieke aard**. Het vaststellen en evalueren van dergelijke risico's van geopolitieke aard vallen buiten het bevoegdheidsdomein van het CCB. Voor veiligheidsgevaren omtrent het gebruik van TikTok, **volgt het CCB daarom het advies van de Veiligheid van de Staat, dat zeer duidelijk is.**

De beste remediërende oplossing, die ook in sommige andere staten eveneens wordt uitgevoerd om tegemoet te komen aan deze geopolitieke risico's, is het aanbevelen tot **niet-gebruik (of zelfs verbod) van de TikTok applicatie op diensttoestellen of toestellen die toegang hebben tot federale overheidsnetwerken -en systemen.**

Conclusie en advies

Een aantal landen informeren hun bevolking rond de privacy risico's verbonden aan het gebruik van TikTok en verbieden de installatie op smartphones van overheidsdiensten.

Het gebruik van producten van Chinese leveranciers is heel complexe materie met veel verschillende invalshoeken en aspecten om rekening mee te houden, maar er is een rode draad in quasi alle dossiers: de risico's zijn niet technisch maar van geopolitieke aard.

Het CCB volgt **de mening van de VSSE ter zake: installeer TikTok niet op apparaten voor professioneel gebruik.**

Er zijn geen bijzondere of uitzonderlijke technische kwetsbaarheden of backdoors vastgesteld in TikTok, maar dat is triviaal. Deze zijn helemaal niet nodig opdat de producent ByteDance toegang zou krijgen tot heel wat gevoelige informatie. Daarenboven zou TikTok data opslaan op servers die onder controle van een Chinese entiteit staan. Het ontbreken van bezwarende technische rapporten of analyses verandert niets aan de veelbesproken risico's die voortvloeien uit het gebruik van TikTok.

Op basis van deze analyse en de informatie van de VSSE adviseert het CCB :

- het gebruik van de TikTok applicatie te verbieden op vaste en mobiele diensttoestellen
- aan te bevelen om TikTok niet te installeren of te gebruiken op persoonlijke toestellen met toegang tot interne federale overheidsnetwerken en -systemen
- de private sector te adviseren om waakzaam te zijn voor de potentiële risico's van het gebruik van TikTok



Adviesrapport TikTok

Bijlage 2: Door het Strategisch Comité voor Inlichting en Veiligheid genomen beslissingen, goedgekeurd door de Nationale Veiligheidsraad



NOTA AAN DE NATIONALE VEILIGHEIDSRaad

9 MAART 2023

NOTA AU CONSEIL NATIONAL DE SECURITE

9 MARS 2023

Betreft: Tijdelijk verbod op het gebruik van TikTok

Uiteenzetting van het dossier

1. Naar aanleiding van onder meer het recente door de Europese Commissie, het Europees Parlement en de Europese Raad ingestelde verbod op het gebruik van de TikTok applicatie op werkgerelateerde toestellen, werd het Centrum voor Cybersecurity België (CCB) gevraagd om, in samenspraak met de inlichtingendiensten, een advies te formuleren.
2. Het adviesrapport in bijlage werd besproken op het Strategisch Comité Inlichtingen en Veiligheid van 8 maart 2023 en in IKW van 9 maart 2023.

Voorstel van beslissing

3. Voor het personeel van de federale overheid¹:
 - a. Verbod, met onmiddellijke ingang, op de installatie en het gebruik van de TikTok applicatie op vaste en mobiele diensttoestellen²;
 - b. Verwijdering, tegen uiterlijk 31 maart 2023, van alle bestaande TikTok applicaties op deze diensttoestellen;
 - c. Aanbeveling om de TikTok applicatie niet te installeren op persoonlijke toestellen

Concerne : Interdiction temporaire d'utiliser TikTok

Exposé du dossier

1. À la suite entre autres de la récente interdiction imposée par la Commission européenne, le Parlement européen et le Conseil européen d'utiliser l'application TikTok sur les appareils liés au travail, le Centre pour la cybersécurité Belgique a été invité à formuler un avis, de concert avec les services de renseignement.
2. Le rapport consultatif ci-annexé a fait l'objet d'une discussion en Comité stratégique du renseignement et de la sécurité le 8 mars 2023 et en GTI le 9 mars 2023.

Proposition de décision

3. Pour le personnel des autorités publiques fédérales³ :
 - a. Interdiction, avec effet immédiat, d'installer et d'utiliser l'application TikTok sur les appareils de service⁴ fixes et mobiles ;
 - b. Suppression, d'ici le 31 mars 2023 au plus tard, de toutes les applications TikTok existantes sur ces appareils de service ;
 - c. Recommandation de ne pas installer

¹ Onder « overheid » wordt verstaan de administraties, instellingen en ondernemingen van de federale Staat zoals gedefinieerd in de wet van 22 mei 2003 houdende organisatie van de begroting en van de comptabiliteit van de federale Staat, het Openbaar Ministerie, Defensie en de federale politie, alsook de regeringsleden en hun beleidscellen.

² Toestellen waarvan de abonnements- of gebruikskosten of aankoop deels of volledig bekostigd worden door de overheid

³ Par « autorités publiques » on entend les administrations, institutions et entreprises de l'État fédéral, telles que définies dans la loi du 22 mai 2003 portant organisation du budget et de la comptabilité de l'État fédéral, le ministère public, la Défense et la Police fédérale, ainsi que les membres du gouvernement et leurs cellules stratégiques.

⁴ Appareils dont les frais d'abonnement ou d'utilisation ou l'achat sont partiellement ou entièrement pris en charge par les pouvoirs publics.

- | | |
|--|--|
| <p>met toegang tot interne federale overheidsnetwerken -en systemen, en om deze te verwijderen indien reeds geïnstalleerd.</p> <p>d. Het CCB wordt verzocht om na te gaan of de webtoegang tot TikTok geblokkeerd kan worden in de professionele omgeving.</p> <p>4. Aan de administraties wordt gevraagd om de toegang tot WiFi-netwerken te differentiëren tussen diensttoestellen en persoonlijke toestellen.</p> <p>5. De gegevensbeschermingsautoriteit wordt verzocht om een onderzoek op te starten naar het privacybeleid van TikTok.</p> <p>6. Maximale verspreiding van het advies van het CCB naar de regionale, provinciale en lokale overheden en instellingen.</p> <p>7. De private sector wordt opgeroepen om waakzaam te zijn voor de potentiële risico's van het gebruik van de TikTok applicatie.</p> <p>8. Het CCB wordt verzocht om na te gaan of het mandaat van de Nationale Raad voor Cyberveiligheid aangepast of uitgebreid moet worden met het oog op technologische en innovatieve waakzaamheid en hierover een advies te formuleren aan het Strategisch Comité Inlichtingen en Veiligheid.</p> <p>9. De Eerste Minister en de Minister van Ambtenarenzaken zullen een ontwerp richtlijn voorleggen aan de Ministerraad voor de uitvoering van dit tijdelijk verbod.</p> <p>10. Het tijdelijk verbod zal geëvalueerd worden na 6 maanden.</p> | <p>l'application TikTok sur les appareils personnels ayant accès aux réseaux et système internes des autorités fédérales, et de la supprimer si elle y est déjà installée ;</p> <p>d. Le CCB est invité à vérifier si l'accès internet à TikTok peut être bloqué dans l'environnement de travail professionnel.</p> <p>4. Les administrations sont invitées à différencier l'accès aux réseaux WiFi entre les appareils de service et les appareils personnels.</p> <p>5. L'autorité de protection des données est invitée à ouvrir une enquête sur la politique en matière de vie privée de TikTok.</p> <p>6. Diffusion maximale de l'avis du CCB auprès des autorités et institutions régionales, provinciales et locales.</p> <p>7. Le secteur privé est appelé à la vigilance quant aux risques potentiels liés à l'utilisation de l'application TikTok.</p> <p>8. Le CCB est invité à vérifier si le mandat du Conseil national de cybersécurité doit être adapté ou élargi en vue d'une veille technologique et d'innovation et de formuler un avis à l'attention du Comité stratégique Renseignement et sécurité.</p> <p>9. Le Premier ministre et la ministre de la Fonction publique soumettront un projet de directive au Conseil des ministres en vue de la mise en œuvre de cette interdiction temporaire.</p> <p>10. L'interdiction temporaire sera évaluée après 6 mois.</p> |
|--|--|

Voorzitter van het Strategisch Comité Inlichtingen en Veiligheid

Le Président du Comité stratégique du renseignement et de la sécurité

Peter MOORS

Bijlage 3: Overzicht per EU-lidstaat van de nationale maatregelen die zijn genomen om de toegang tot de app TikTok te beperken

De lidstaten worden in vier categorieën ingedeeld op basis van de informatie die op 31 maart 2023 via open source beschikbaar is. De informatie moet met de nodige voorzichtigheid worden gelezen, daar het om een actuele problematiek gaat in verband waarmee verschillende landen hebben laten verstaan dat ze in de nabije toekomst nationale maatregelen zouden kunnen nemen of dat de al genomen maatregelen zouden kunnen evolueren.⁵⁴

Het gaat om de volgende categorieën:

- Verbodsmatregelen: Landen waar verbodsmatregelen zijn genomen. De draagwijdte en het niveau van de maatregelen verschillen sterk van land tot land.
- Aanbevelingen: Landen waar aanbevelingen zijn geformuleerd.
- Geen beperkingen: Landen waar geen beperkingen zijn opgelegd of meegedeeld (inclusief aanbevelingen).
- Onbekend: Landen waarover geen informatie beschikbaar is.

LAND	CATEGORIE	INFORMATIE
DUITSLAND	Verbodsmatregelen	In Duitsland is er geen gemeenschappelijk beleid voor alle ministeries. Elk ministerie kan zelf kiezen of het de toegang tot TikTok wil beperken of niet. Sommige ministeries hebben een restrictief beleid uitgewerkt. Zo beperkt het ministerie van Defensie de toegang tot de app sinds 2020. Binnen het ministerie van Binnenlandse Zaken is het niet mogelijk toegang te krijgen tot de app of om de app te installeren op de officiële diensttelefoons. Andere ministeries hebben (nog) geen standpunt ingenomen. ⁵⁵
OOSTENRIJK	Geen beperkingen	De Oostenrijkse regering verklaarde in maart 2023 dat een risicoanalyse onder leiding van het ministerie van Binnenlandse Zaken aan de gang was om te bepalen of er beperkende maatregelen moeten worden genomen. ⁵⁶
BULGARIJE	Onbekend	
CYPRUS	Onbekend	

⁵⁴ In dit verband heeft het Vast Comité I op 6 april 2023 contact opgenomen met de Belgische ambassades in Hongarije, Cyprus en Bulgarije om het standpunt van de buitenlandse regeringen ter zake te vernemen. Tot op heden is er geen reactie op de e-mails gekomen.

⁵⁵ Politico, "Mapped: TikTok faces bans, blocks and probes across Europe", 5 maart 2023.

⁵⁶ Vienna Times, "Austria Considers Banning TikTok Over Security Concerns", 3 maart 2023; The Storiest, "TikTok ban for Austria's officials? decision before Easter", 24 maart 2023.

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

KROATIË	Onbekend	
DENEMARKE	Verbodsmaatregelen	<p>Eind februari 2023 publiceerde het Deense centrum voor cyberveiligheid (CFCS) een communiqué waarin overheidsmedewerkers het advies kregen om de app TikTok niet op hun diensttoestellen te installeren. Naar aanleiding van dit advies heeft het Deense parlement zijn leden en personeel afgeraden de app te gebruiken.⁵⁷</p> <p>Op 6 maart 2023 besliste het ministerie van Defensie om de installatie en het gebruik van TikTok te verbieden op de diensttoestellen van zijn medewerkers.⁵⁸</p>
SPANJE	Geen beperkingen	Eind maart 2023 had de Spaanse regering nog geen standpunt ingenomen over mogelijke beperkingen op het gebruik van TikTok door overheidspersoneel. ⁵⁹
ESTLAND	Aanbevelingen	<p>De Estse informatiecontroleautoriteit (RIA) heeft de overheden aanbevolen om TikTok enkel te gebruiken op toestellen die niet voor beroepsmatig gebruik zijn bestemd. De toezichthouder zelf heeft zijn personeel verboden de app te gebruiken. Zonder dat een verbod werd afgekondigd, lieten vijf ministeries weten dat hun personeel TikTok niet gebruikte op diensttoestellen.⁶⁰</p> <p>Op 29 maart 2023 liet de minister bevoegd voor informatietechnologie verstaan dat het de bedoeling was een verbod af te kondigen op het gebruik van TikTok op de officiële toestellen van overheidsmedewerkers.⁶¹</p>
FINLAND	Verbodsmaatregelen	Er is geen algemeen verbod voor overheidspersoneel. Het ministerie van Defensie heeft een verbod uitgevaardigd voor zijn personeel om TikTok te installeren en te gebruiken op diensttoestellen. ⁶²
FRANKRIJK	Verbodsmaatregelen	Op 24 maart 2023 verbood de Franse regering de installatie en het gebruik van zogenaamde "recreatieve" apps zoals TikTok of het Amerikaanse streamingplatform Netflix op de diensttelefoons van de ambtenaren van alle ministeries. Na een analyse door het Agence nationale de la sécurité des systèmes d'information (Anssi, nationaal agentschap voor de veiligheid

⁵⁷ Euroactiv, "TikTok : le parlement danois n'en veut plus", 1 maart 2023.

⁵⁸ The Associated Press, "Danish defense ministry bans TikTok on employee work phones", 6 maart 2023.

⁵⁹ Esquire, "¿TikTok podría prohibirse en España?", 17 maart 2023.

⁶⁰ Baltic News Network, "Legislative changes needed to completely ban TikTok in Estonia", 3 maart 2023; Eesti Rahvusringhääling, "Complete Tiktok ban in Estonia difficult without amending law", 3 maart 2023.

⁶¹ Eesti Rahvusringhääling, "Minister Järvan: TikTok to be banned on state officials' work phones", 29 maart 2023.

⁶² TimeNews, "Swedish Work Mobile Phones Not Allowed to Use Tiktok by the Armed Forces", 27 maart 2023; The Defence Post, "Swedish Military Bans Chinese-Owned Tiktok on Work Phones", 28 maart 2023.

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

		<p>van informatiesystemen) en de Direction interministérielle du numérique (Dinum, interministeriële directie voor digitale zaken) kwam de regering tot het besluit dat "recreatieve" apps "<i>risico's [inhielden] op het vlak van cyberveiligheid en de bescherming van de gegevens van ambtenaren en de administratie</i>". Tot op heden werd nog <i>geen enkele</i> lijst van apps opgesteld, maar wel staat vast dat drie grote categorieën van apps in de ban zullen worden geslagen, i.e. spelletjesapps (bv. <i>Candy Crush</i>), streamingapps (bv. Netflix) en recreatieve apps (bv. TikTok). Er kunnen slechts enkele individuele vrijstellingen kunnen worden verleend voor bijvoorbeeld institutionele communicatiedoelstellingen. Het verbod is onmiddellijk van kracht geworden en heeft geen gevolgen voor de persoonlijke telefoons van de ambtenaren.⁶³</p> <p>Tegelijk heeft de Franse Senaat op 6 maart 2023 een commissie gecreëerd die de opdracht heeft gekregen een onderzoek te voeren naar het gebruik van het sociale netwerk TikTok, naar de manier waarop het gegevens exploiteert en naar zijn beïnvloedingsstrategie, i.e. "<i>Commission d'enquête sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence</i>". De Commissie heeft haar kalender nog niet bekendgemaakt, maar heeft haar werkzaamheden aangevat op 11 maart 2023.⁶⁴</p>
GRIEKENLAND	Onbekend	
HONGARIJE	Onbekend	
IERLAND	Geen beperkingen	<p>Eind maart 2023 kondigde de Ierse regering aan dat, na een grondige analyse van de veiligheidsrisico's in verband met het gebruik van TikTok en andere apps van sociale media op telefoontoestellen, nieuwe richtlijnen voor de diensttelefoons van de ministers en ambtenaren zouden worden gepubliceerd tijdens "<i>de komende weken</i>".⁶⁵</p> <p>Op te merken valt dat de app in het verleden al aanleiding had gegeven tot bezorgdheid inzake de bescherming van de gegevens van de gebruikers van de app, als gevolg waarvan de Ierse Autoriteit voor de bescherming van de persoonlijke</p>

⁶³ Le Monde, "*TikTok, Netflix et autres « applications récréatives » interdites sur les téléphones professionnels des fonctionnaires d'Etat français*", 24 maart 2023; Franceinfo, "*Le gouvernement interdit les « applications récréatives », dont TikTok, Instagram et Twitter, sur les téléphones des fonctionnaires d'Etat*", 24 maart 2023; Euroactiv, "*TikTok et Netflix interdits sur les portables des fonctionnaires français*", 24 maart 2023.

⁶⁴ Commission d'enquête sur l'utilisation du réseau social Tiktok, son exploitation des données, sa stratégie d'influence - Senaat (senat.fr).

⁶⁵ Irish Mirror, "*TikTok could be banned on Irish politicians' phones over security concerns*".

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

		levenssfeer in september 2021 had beslist om twee onderzoeken te openen naar de app: het eerste had tot doel na te gaan op welke manier TikTok informatie verzamelt met betrekking tot minderjarige gebruikers, het tweede focuste op de doorgifte door TikTok van persoonsgegevens naar China. ⁶⁶
ITALIË	Geen beperkingen	In februari 2023 was de politieke wereld verdeeld over het feit of TikTok al dan niet moest worden beperkt op de toestellen van ambtenaren. Er werden geen maatregelen genomen om de toegang tot de app te beperken. Op 21 maart 2023 werd door de Italiaanse mededingingsautoriteit een onderzoek tegen het netwerk ingesteld wegens "gevaarlijke inhoud" op de app. Samen met de financiële politie ging voornoemde autoriteit over tot een inspectie in het Italiaanse hoofdkantoor van TikTok. ⁶⁷
LETLAND	Verbodsmaatregelen	In Letland zijn verbodsmaatregelen genomen door het ministerie van Buitenlandse Zaken, dat op 2 maart 2023 om veiligheidsredenen het gebruik van het platform op de officiële toestellen van zijn ambtenaren heeft verboden. Andere ministeries zouden overwegen om soortgelijke maatregelen te nemen. ⁶⁸
LITOUWEN	Geen beperkingen	Begin maart 2023 liet de Litouwse regering weten niet van plan te zijn maatregelen te nemen om het gebruik van de app door haar ambtenaren te verbieden. ⁶⁹
LUXEMBURG	Geen beperkingen	Eind maart 2023 had de Luxemburgse regering geen maatregelen getroffen om de toegang tot TikTok voor haar ambtenaren te beperken. Het Groothertogdom zou, samen met andere lidstaten, de Europese Commissie om nadere informatie hebben gevraagd met betrekking tot de redenen voor de beperkingen die aan EU-ambtenaren zijn opgelegd. ⁷⁰

⁶⁶ Le Figaro, "TikTok visé en Irlande par deux enquêtes sur sa gestion des données personnelles", 15 september 2021.

⁶⁷ Deutsche Welle, "Italy investigates TikTok over 'dangerous content'", 21 maart 2023; L'avenir, "'Un tournant pour TikTok': le réseau menacé d'interdiction aux USA, déconseillé aux Pays-Bas, sous enquête en Italie", 21 maart 2023.

⁶⁸ LSM, "Latvian Foreign Ministry bans TikTok on work phones", 2 maart 2023.

⁶⁹ The Baltic Times, "Lithuanian authorities don't plan to ban TikTok, but advise against using it – official", 28 februari 2023; LRT, "Lithuania won't ban TikTok from official devices", 28 februari 2023.

⁷⁰ RTL, "Pour le moment, les fonctionnaires luxembourgeois peuvent utiliser l'appli", 29 maart 2023.

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

MALTA	Verbodsmaatregelen	Op Malta is de app TikTok niet toegankelijk op alle officiële apparaten, net als alle andere niet-overheidsapplicaties, tenzij de gebruiker uitgebreide toegang tot het internet heeft. ⁷¹
NEDERLAND	Aanbevelingen	Op basis van een advies van de Nederlandse inlichtingendienst AIVD ⁷² besliste de regering op 21 maart 2023 om haar ambtenaren sterk af te raden TikTok of andere apps die worden beheerd door landen met een "offensief cyberprogramma" te gebruiken op hun diensttoestellen. Volgens de AIVD bestaat er "een verhoogd risico van spionage" via het gebruik op de diensttelefoons van de ambtenaren van TikTok of andere apps die worden beheerd door landen met een offensief cyberprogramma zoals Rusland, China, Iran en Noord-Korea. De Nederlandse regering verklaarde ook nog te zoeken naar een structurele oplossing om de installatie van deze apps onmogelijk te maken op de diensttelefoons van overheidspersoneel. ⁷³
POLEN	Geen beperkingen	<p>Begin maart 2023 verklaarde de Poolse regering dat er geen beperkende maatregelen in overweging werden genomen en dat de regering de app overigens zou blijven gebruiken als overheidsinstrument, ook voor verkiezingsdoeleinden. De Poolse regering heeft aan de Europese Commissie ook gevraagd om nadere toelichting te verstrekken bij haar beslissing om de socialenetwerkkapp te verbieden op de telefoons van haar personeel.⁷⁴</p> <p>Eind maart 2023 heeft een adviesorgaan van de Poolse regering aanbevolen het gebruik van de app op de werktelefoons van overheidspersoneel te verbieden.⁷⁵</p>
PORTUGAL	Geen beperkingen	Eind maart 2023 had Portugal nog geen officieel standpunt ingenomen of maatregelen getroffen om het gebruik van de app TikTok door ambtenaren te verbieden of te beperken. ⁷⁶

⁷¹ MaltaToday, "TikTok blocked on government devices just like other social networking sites", 16 maart 2023.

⁷² Algemene Inlichtingen- en Veiligheidsdienst, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, "De Beschouwing risico's gebruik applicaties uit landen met een offensief cyberprogramma gericht tegen Nederland", 23 februari 2023 : Beschouwing risico's gebruik applicaties landen met offensief cyberprogramma gericht tegen Nederland | Brief | Rijksoverheid.nl

⁷³ Nieuwsblad, « Ook Nederlandse regering roept ambtenaren nu op om TikTok te verwijderen van werktelefoon », 21 maart 2023 ; Euroactiv, "TikTok et les applications « à risque d'espionnage » interdites sur les appareils des fonctionnaires néerlandais", 22 maart 2023.

⁷⁴ Euroactiv, "La Pologne va continuer à utiliser TikTok et remet en question l'interdiction de l'UE", 3 maart 2023.

⁷⁵ Reuters, "Polish council recommends banning TikTok on public administration phones – media", 27 maart 2023.

⁷⁶ Espresso, "O TikTok vai ser banido nos EUA? E em Portugal? E haverá realmente perigo? Para quem? 10 perguntas e respostas sobre a polémica", 24 maart 2023.

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

TSJECHISCHE REPUBLIEK	Aanbevelingen	Op 8 maart 2023 publiceerde het nationaal Tsjechisch centrum voor cyberveiligheid en informatiebeveiliging (NUKIB) een bindende officiële waarschuwing voor personen en entiteiten die aan de Tsjechische wet inzake cyberveiligheid zijn onderworpen: <i>"Based on the warning, obliged persons must respond by taking appropriate security measures. This threat is assessed as "High", meaning probable to very probable. The NÚKIB recommends prohibiting the installation and use of TikTok on devices that have access to the regulated system (corporate devices as well as personal devices used for work purposes) as the best way to eliminate or minimize the threat. The Agency also encourages the public to reconsider using TikTok as well as the quantities and types of data that they share through the app. We do not recommend using the app to "persons of interest" who hold high-level political, public, or decision-making positions. The warnings issued and the recommendations outlined above are in accordance with the Cyber Security Act, which requires NÚKIB to promote prevention in the field of cyber security."</i> ⁷⁷
ROEMENIË	Geen beperkingen	Op 2 maart 2023 deelde de Roemeense minister bevoegd voor digitalisering mee dat de Roemeense autoriteiten een analyse waren begonnen om na te gaan of de app TikTok, die destijds zelfs door parlementsleden en openbare instellingen zonder verbod werd gebruikt, een veiligheidsrisico vormt, en dat pas op basis van een volledige analyse mogelijke maatregelen zouden worden genomen. ⁷⁸
SLOWAKIJE	Aanbevelingen	Er is geen algemene maatregel om de app te verbieden of het gebruik ervan te beperken. Niettemin formuleerde het ministerie van Binnenlandse Zaken op 14 maart 2023 voor zijn medewerkers de aanbeveling om TikTok bij wijze van voorzorgsmaatregel niet te installeren of te gebruiken, wegens het bestaan van een ernstige cyberdreiging, op de diensttoestellen en de apparaten die toegang hebben tot de informatie- en communicatiesystemen van het ministerie van Binnenlandse Zaken. ⁷⁹

⁷⁷ National Cyber and Information Security Agency - The TikTok app poses a security threat (nukib.cz); Euroactiv, "TikTok représente une menace sécuritaire pour la République tchèque", 9 maart 2023.

⁷⁸ Romania Insider, "Romania to check whether TikTok poses security issues", 2 maart 2023.

⁷⁹ Euroactiv, "Slovak Interior Ministry recommends employees delete TikTok", 15 maart 2023.

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSKOMMISSIE

SLOVENIË	<i>Aanbevelingen</i>	Op 10 maart 2023 formuleerde het bureau voor informatiebeveiliging van de regering een aanbeveling dat Sloveense ambtenaren het TikTok-platform niet op hun werktelefoon mogen gebruiken vanwege de risico's voor de cyberveiligheid. ⁸⁰
-----------------	----------------------	---

⁸⁰ Slovenia Times, "Civil servants urged not to use TikTok", 10 maart 2023.

Bijlage 4 : Korte synthese van de technische analyses van Citizen Lab en Check Point over TikTok & Onderzoeken Data Protection Commission (Ierland)

In de antwoorden die de ADIV en de VSSE hebben meegedeeld aan het CCB in het kader van een advies betreffende het gebruik van de applicatie TikTok op apparaten gebruikt door functionarissen door de federale overheid, citeren zij respectievelijk analyserapporten die werden opgesteld door twee onderzoeksbureaus. Dit zijn Citizen Lab en Checkpoint.^{81 82} Het feit dat de diensten deze rapporten expliciet vermelden, wijst erop dat zij deze significant, relevant en betrouwbaar achten.

Het rapport van Citizen Lab, dat dateert van maart 2021, bevat een vergelijkende analyse op het vlak van (cyber)veiligheid, privacy-issues en censuur op de platformen TikTok en Douyin. Douyin is een sociaal mediaplatform dat eveneens eigendom is van ByteDance, het Chinese moederbedrijf van TikTok. Dit platform wordt gecommmercialiseerd in China zelf en in andere landen in Zuid-Oost Azië.

Het rapport van Citizen Lab somt een aantal 'key findings' op:⁸³

- TikTok en Douyin lijken geen openlijk kwaadaardig gedrag te vertonen dat lijkt op malware. Er zijn geen aanwijzingen waargenomen dat beide apps contactlijsten, foto's, audio- en videobestanden of geolocatiecoördinaten verzamelen en versturen zonder toestemming van de gebruiker.
- Hoewel Douyin geen kwaadaardig gedrag vertoont, bevat het functies die privacy- en veiligheidsproblemen opleveren, zoals het dynamisch laden van code en zoekcensuur aan de serverzijde. TikTok bevat deze functies niet.
- De Android-apps van TikTok en Douyin delen veel van hun broncode. Er kan worden verondersteld dat ByteDance TikTok en Douyin ontwikkelt op basis van een gemeenschappelijke codebasis en verschillende aanpassingen toepast volgens de behoeften van de markt. Er werd geconstateerd dat sommige van deze aanpassingen kunnen worden in- of uitgeschakeld door verschillende van de server teruggestuurde

⁸¹ Citizen Lab omschrijft zichzelf als *"een interdisciplinair laboratorium verbonden gevestigd aan de Munk School of Global Affairs & Public Policy, University of Toronto, gericht op onderzoek, ontwikkeling en strategische beleids- en juridische betrokkenheid op hoog niveau op het snijvlak van informatie- en communicatietechnologieën, mensenrechten en mondiale veiligheid.*

Wij gebruiken een "gemengde" onderzoeksmethode die methoden uit de politieke wetenschappen, het recht, de computerwetenschappen en gebiedsstudies combineert. Ons onderzoek omvat het onderzoeken van digitale spionage tegen de burgermaatschappij, het documenteren van internetfiltering en andere technologieën en praktijken die de vrijheid van meningsuiting online beïnvloeden, het analyseren van privacy-, veiligheids- en informatiecontroles van populaire toepassingen, en het onderzoeken van transparantie- en verantwoordingsmechanismen die relevant zijn voor de relatie tussen bedrijven en overheidsinstellingen met betrekking tot persoonsgegevens en andere bewakingsactiviteiten."

⁸² Check Point Software Technologies Ltd. is een van oorsprong Israëliëse, multinationale privéonderneming die leverancier is van cyberbeveiligingsoplossingen voor bedrijven en overheden wereldwijd. Het heeft een onderzoeksafdeling die informatie over cyberdreigingen levert aan klanten van het bedrijf en aan de ruimere inlichtingengemeenschap. Deze onderzoeksafdeling bestaat uit 150 analisten en onderzoekers die samenwerken met andere cyberbeveiligingsfirma's, veiligheidsdiensten en CERT's (Cyber Emergency Response Team).

⁸³ *"TikTok vs Douyin – A Security and Privacy Analysis"*, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto, March 22, 2021, 71p.

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSCOMMISSIE

configuratiewaarden. Er bestaat een onbevestigde vrees dat deze mogelijkheid kan worden gebruikt om privacyschendende verborgen functies in te schakelen.

- Zowel TikTok als Douyin bevatten broncode voor het beperken van zoekresultaten voor inhoud die in verband wordt gebracht met "hate speech", "zelfmoordpreventie", of die als "gevoelig" wordt beschouwd. Het vermoeden bestaat dat "gevoelig" verwijst naar "politiek gevoelig", maar dit kan niet worden bevestigd.
- Het verzamelde bewijsmateriaal geeft geen uitsluitsel over de vraag of TikTok politieke censuur toepast op berichten van gebruikers.
- Douyin beperkt sommige politieke termen bij het zoeken. TikTok beperkte geen van de geteste trefwoorden.

Het rapport gaat nog verder in op de aspecten van privacy, (cyber)veiligheid en censuur.

Wat betreft het aspect **privacy**, bevat het rapport de resultaten van de analyse van dataverkeer, en laat het zien welke gegevens de toepassingen verzamelen en wanneer ze worden verzonden, en naar welke bestemmingen ze worden gestuurd. In het algemeen werd vastgesteld dat geen van beide toepassingen zonder toestemming gevoelige persoonsgegevens lijkt te verzamelen (bv. contactlijsten, gebruikersbestanden of geolocatiecoördinaten). Douyin bevat veel functies die ongeschikt zijn voor de internationale markt, zoals het dynamisch laden van code en zoekcensuur aan de serverzijde. TikTok bevat deze functies niet. TikTok verzamelt een grote verscheidenheid aan apparaatinformatie en informatie over het gebruikspatroon. Het maakt ook gebruik van advertentie- en volgdiensten van derden, waaronder Facebook, Firebase Analytics en AppsFlyer. Deze kenmerken zijn niet uitzonderlijk in vergelijking met de industrienormen.

Op het vlak van **(cyber)veiligheid** blijkt uit de analyse van de broncode dat TikTok en Douyin geen duidelijk kwaadaardig gedrag vertonen. Er werd niet waargenomen dat een van beide apps contactlijsten verzamelt, foto's, audio, video's of geolocatiecoördinaten opneemt en/of verstuurt zonder toestemming van de gebruiker. Douyin bevat veel functies die gebruikers op de internationale markt ongewenst kunnen vinden, zoals het dynamisch laden van code en zoekcensuur aan de serverzijde. TikTok bevat deze functies niet.

Qua **censuur** tenslotte rapporteert Citizen Lab over de analyse van post- en zoekcensuur op TikTok en Douyin. Op basis van de resultaten is het onduidelijk of TikTok politieke censuur toepast op berichten van gebruikers. Er werd niet getest op postcensuur op Douyin. Zowel TikTok als Douyin hebben broncode voor server-side zoekcensuur, waarmee zoekresultaten kunnen worden beperkt voor inhoud met het label "haatzaaien", "zelfmoordpreventie" en "gevoelig". Er is een vermoeden dat de "gevoelige" beperking verwijst naar inhoud die "politiek gevoelig" is, maar dit kon niet worden bevestigd. Douyin beperkt sommige politieke termen bij het zoeken. TikTok heeft geen van de geteste zoektermen beperkt.

Het tweede onderzoeksrapport dat door met name de VSSE werd vermeld, betreft een (cyber)veiligheidsanalyse, uitgevoerd door Check Point, waarvan de resultaten online werden gepubliceerd begin januari 2020.⁸⁴

⁸⁴ "Tik or Tok? Is TikTok Secure Enough?", Check Point, January 8, 2020. <https://research.checkpoint.com/2020/tik-or-tok-is-tiktok-secure-enough/>

VERTROUWELIJK TOT AAN DE VERGADERING MET DE BEGELEIDINGSKOMMISSIE

De technische analyse van Check Point legde een aantal kwetsbaarheden bloot van de app, waardoor volgende misbruiken mogelijk werden:

- Controle verwerven over (andermans) TikTok-accounts en de inhoud ervan manipuleren;
- Het ongewenst verwijderen en uploaden van videobestanden;
- Het ongewenst openbaar maken van “verborgen” privévideo’s;
- Het ongevraagd bekendmaken van persoonlijke informatie – zoals e-mailadressen - die in een account zijn opgeslagen.

Op 26 januari 2021 maakte Check Point op zijn website bekend dat de kwetsbaarheden die het bedrijf in de TikTok-app had ontdekt, werden gedeeld met TikTok, en dat TikTok de nodige stappen had ondernomen om deze kwetsbaarheden aan te pakken en recht te zetten.⁸⁵ In april 2020 lanceerde TikTok een particulier bug bounty-programma⁸⁶ dat in oktober 2020 uitgroeide tot een wereldwijd publiek partnerschap met HackerOne en dat beveiligingsonderzoekers aanmoedigt om beveiligingsbugs te vinden en op verantwoorde wijze openbaar te maken.

De vraag of het gebruik van de TikTok-app belangrijkere problemen op het vlak van veiligheid en privacy (bescherming van persoonsgegevens) met zich meebrengt dan bij het gebruik van andere applicaties en/of sociale mediaplatformen, wordt in grote mate bepaald door het antwoord op de vraag of het bedrijf gegevens doorstuurt en/of opslaat in China.

Op 14 september 2021 kondigde de Data Protection Commission (DPC) van Ierland aan dat het twee onderzoeken zou instellen naar de naleving door TikTok Technology Limited van de vereisten van de Europese GDPR-verordening.⁸⁷

Het eerste onderzoek betreft de naleving door TikTok van de GDPR-gegevensbescherming voor zover deze betrekking hebben op de verwerking van persoonsgegevens in het kader van platforminstellingen voor gebruikers onder de 18 jaar en leeftijdsverificatiemaatregelen voor personen onder de 13 jaar. In dit onderzoek werd nagegaan of TikTok heeft voldaan aan de transparantieplichtingen van de GDPR in het kader van de verwerking van persoonsgegevens van gebruikers jonger dan 18 jaar.

13 september 2022 meldde de DPC dat dit eerste onderzoek was afgerond en dat een ontwerpbesluit van dit onderzoek werd voorgelegd aan andere betrokken toezichthoudende autoriteiten in de EU.⁸⁸

Het tweede onderzoek van de DPC is gericht op de overdracht van persoonsgegevens door TikTok aan China en de naleving door TikTok van de vereisten van de GDPR voor de overdracht van persoonsgegevens aan derde landen.

Het is het Vast Comité I niet bekend of dit tweede onderzoek reeds werd afgerond, of wanneer hierover zal gerapporteerd worden.

⁸⁵ <https://blog.checkpoint.com/security/tiktok-fixes-privacy-issue-discovered-by-check-point-research/>

⁸⁶ Een bug bounty-programma looft beloningen uit aan ethische hackers om kwetsbaarheden in systemen op te sporen, en te melden aan de beheerder.

⁸⁷ <https://www.dataprotection.ie/en/news-media/latest-news/dpc-launches-two-inquiries-tiktok-concerning-compliance-gdpr-requirements-relating-processing>

⁸⁸ <https://www.dataprotection.ie/en/news-media/irish-dpc-submits-article-60-draft-decision-inquiry-tiktok-0>