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

CENTRE FOR
CYBER SECURITY
BELGIUM

# Inhoudstabel

CENTRE FOR CYBER SECURITY BELGIUM

## 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 doorgeklikt 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 104millioen 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 experten.

**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 ligt 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 €5millioen, 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, Azerbaijan,

[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 gespecifieerde '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.*

*…*

<u>Met betrekking tot Chinese smartphones vermeldt de VSSE het volgende:</u>

*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.*

<u>Opmerking bij de input van VSSE</u>

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 dienstreden 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

CENTRE FOR
CYBER SECURITY
BELGIUM

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.**

CENTRE FOR
CYBER SECURITY
BELGIUM

## 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

CENTRE FOR
CYBER SECURITY
BELGIUM

# Adviesrapport TikTok