



CENTRE FOR  
**CYBER SECURITY**  
BELGIUM



CENTRE FOR  
**CYBER SECURITY**  
BELGIUM

# Rapport avis TikTok

(8 mars 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

## Table des matières

<i>Contexte</i> .....	2
<i>Le défi des « open sources »</i> .....	3
<i>Réactions internationales</i> .....	4
États Unis .....	4
Europe .....	5
Ailleurs dans le monde .....	6
<i>Contribution de la VSSE</i> .....	7
<i>Contribution du SGRS</i> .....	9
<i>Analyse technique du CCB</i> .....	10
<i>Conclusion et avis</i> .....	11

### Contexte

TikTok est un service qui héberge des courtes vidéos, lesquelles peuvent être réalisées, montées et envoyées via l'application TikTok sur smartphone pour que les autres utilisateurs puissent ensuite les visionner. Les utilisateurs reçoivent ces vidéos sur leur fil d'actualité en fonction de leur activité personnelle sur l'application. Il est également possible d'utiliser un navigateur pour parcourir le contenu proposé.

Le service a été lancé en septembre 2016, en Chine, sous le nom de « Douyin » et a été proposé en tant que service et application distincts sur le marché international à partir de septembre 2017, dans plus de 75 langues. Selon la société d'analyse Sensor Tower, l'application a été installée pas moins de 104 millions de fois la première année et, à la fin février 2023, elle avait été téléchargée 3,5 milliards de fois dans le monde.

Le service est détenu par la société chinoise de technologie internet ByteDance, qui a son siège à Pékin.

### Le défi des « open sources »

Au vu de son immense popularité et du fait qu'elle est mise à disposition par une entreprise chinoise, l'application TikTok a vite attiré l'attention des autorités régulatrices, des défenseurs de la vie privée et des experts en sécurité nationale.

### **Les inquiétudes entourant l'application concernent notamment trois aspects liés mais toutefois distincts : la collecte de données, le partage avec les autorités et l'influence.<sup>1</sup>**

Parmi les « open sources », d'aucuns pensent que TikTok **collecte des données des utilisateurs**, notamment leur localisation, le type de leur smartphone, leur comportement sur l'application et sur les sites Internet atteints via l'application dans le navigateur TikTok, ce qui pourrait permettre la collecte de numéros de cartes de crédit et de mots de passe.<sup>2</sup> Selon certains chercheurs, cette collecte de données se ferait à grande échelle et sans le consentement explicite des utilisateurs, ce qui s'inscrit en porte-à-faux du Règlement général sur la protection des données (RGPD). La protection de la vie privée des mineurs, qui constituent un groupe très important d'utilisateurs, suscite également des inquiétudes. TikTok nie toutes ces allégations et, selon d'autres enquêteurs, TikTok ne ferait rien de tout cela, contrairement à d'autres plateformes de médias sociaux similaires. Toutefois, certaines autorités chargées de la protection des données ont déjà infligé des amendes à TikTok en raison des politiques vagues en matière de traitement des données à caractère personnel (voir le point « Réponse internationale » ci-dessous).

Les analystes internationaux soulignent que la **loi chinoise de 2017 sur le renseignement national** stipule que toutes les organisations chinoises et tous les citoyens chinois sont légalement tenus de

---

<sup>1</sup> [https://www.bbc.com/news/technology-64797355?at\\_medium=RSS&at\\_campaign=KARANGA](https://www.bbc.com/news/technology-64797355?at_medium=RSS&at_campaign=KARANGA)

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

soutenir, d'assister et de coopérer avec les agences de renseignement chinoises. Certains médias ont également rapporté que certains employés de l'application pourraient bel et bien avoir eu accès aux données des utilisateurs. TikTok a répondu qu'il s'agissait de cas individuels et certains chercheurs ont nuancé la force juridique des obligations énoncées dans la loi sur le renseignement en ce qui concerne ce type de partage de données. TikTok/ByteDance continue d'affirmer ne jamais avoir procédé et ne jamais procéder à un tel partage de données et que les données ne seraient par ailleurs pas stockées en Chine.

TikTok est l'une des rares plateformes de médias sociaux populaires à ne pas être sous le joug des entreprises américaines. La grande popularité de l'application suscite donc des inquiétudes, notamment en matière d'espionnage, et plus spécifiquement envers le personnel des services publics qui utiliserait l'application.

Enfin, selon des sources publiques, on craint que TikTok, et par extension les pouvoirs publics chinois, ne **contrôlent l'algorithme** qui détermine le contenu que les utilisateurs peuvent voir ou ne pas voir sur l'application. Si les chercheurs sont divisés sur la question de savoir si TikTok procède réellement à une telle censure et une telle influence, il est en théorie possible de le faire, comme sur de nombreuses plateformes de médias sociaux.

Par ailleurs, l'effet que TikTok, en tant que plateforme de médias sociaux, pourrait avoir sur le comportement des utilisateurs (et sur leur comportement d'acheteur) reste une préoccupation générale. Les mineurs – un groupe vulnérable et vaste d'utilisateurs – constituent une préoccupation majeure à cet égard. Bien entendu, à l'instar des autres médias sociaux, d'autres acteurs comme la Russie peuvent utiliser la plateforme à des fins de propagande. Grâce à l'algorithme qui s'appuie sur les intérêts des utilisateurs, les visiteurs de l'application pourraient être de plus en plus piégés dans un récit unique, sans disposer d'aucune alternative.

Toutes ces préoccupations sont principalement renforcées par les tensions géopolitiques croissantes entre les États-Unis et la Chine et ce, dans de nombreux domaines.

## Réactions internationales

### États Unis

Il n'est pas surprenant que la réaction la plus virulente à l'éventuelle menace que constituerait TikTok soit venue jusqu'à présent des États-Unis. Des enquêteurs ont identifié la plateforme comme une

menace pour la sécurité nationale du pays, dans la même veine que Huawei.<sup>3</sup> Plusieurs représentants politiques ont demandé des enquêtes et, en août 2020, le président Trump a pris des mesures pour introduire une interdiction générale de TikTok si la plateforme n'était pas vendue. L'interdiction a été bloquée par les tribunaux.

Le gouvernement du président Biden a retiré la demande du président Trump en juin 2021, tout en lançant une enquête sur le risque que constitue l'application pour la sécurité nationale.

En juin 2022, le commissaire de la FCC a demandé à Apple et à Google de ne plus proposer TikTok sur leurs appstores, craignant que le service ne collecte les données des citoyens.

Récemment, le président Biden a émis un décret stipulant que TikTok devait être supprimé de tous les appareils des autorités fédérales dans les 30 jours. Plusieurs États américains ont également émis des décrets similaires.

## Europe

Au cours des derniers mois, l'Europe s'est montrée plus ferme sur les dangers potentiels de l'application. Dans un premier temps, des amendes ont été imposées à TikTok en raison de la faiblesse des politiques de confidentialité. En outre, à l'instar des États-Unis, l'on s'attarde actuellement à interdire l'application sur les appareils des services publics.<sup>4</sup>

En juillet 2021 déjà, l'autorité de protection des données (APD) néerlandaise a infligé à TikTok une amende de 750 000 euros pour atteinte à la vie privée de mineurs. L'autorité a recommandé de ne pas utiliser l'application jusqu'à ce qu'elle modifie sa politique de protection des données. L'APD irlandaise est en train de finaliser une autre enquête sur les mêmes pratiques. En décembre 2022, l'APD française (CNIL) a également infligé une amende de 5 millions d'euros à TikTok, car les utilisateurs de tiktok.com ne pouvaient pas facilement refuser les cookies et n'étaient pas suffisamment informés de l'utilisation de ces cookies.<sup>5</sup>

---

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

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

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

Certains États membres et institutions européennes ont imposé une véritable interdiction d'utilisation de l'application.

- La **Finlande** a déjà ordonné aux fonctionnaires de supprimer l'application de leurs appareils professionnels en août 2022.

- L'**Estonie** a également interdit aux employés du ministère de la défense d'installer l'application, non seulement sur leurs appareils professionnels, mais **aussi sur leurs appareils personnels**.

Fin février 2023, la **Commission européenne**, rapidement suivie par le **Service européen pour l'action extérieure**, le **Parlement européen** et le **Conseil de l'UE**, a interdit à ses collaborateurs d'utiliser l'application sur les appareils liés à leur travail.<sup>6</sup>

D'autres États membres sont moins stricts :

- Au **Danemark**, le président du parlement et le centre pour la cybersécurité national recommandent vivement à leurs collaborateurs de supprimer l'application de leurs téléphones, du moins ceux destinés à un usage professionnel.
- En **Allemagne**, il n'y a pas de directives générales et c'est à chaque service public de se prononcer concernant l'utilisation de l'application. Le ministère allemand de la défense a déjà limité l'utilisation de l'application depuis 2020. Au sein du ministère de l'intérieur, l'application est inaccessible et son installation sur les téléphones professionnels officiels a été rendue techniquement impossible. L'agence allemande de cybersécurité BSI a émis des avis.

La plupart des États membres, comme **la Lettonie, l'Espagne, l'Irlande, la Pologne, la France, l'Italie et les Pays-Bas**, continuent toutefois d'évaluer leur position et suivent l'évolution de la situation aux niveaux national et européen, avec ou sans enquêtes techniques en cours par les autorités de protection des données sur les politiques de TikTok.

En France, le Sénat a déjà exprimé sa volonté de mener sa propre enquête sur l'utilisation abusive des données et les stratégies d'influence de TikTok. Le président français Emmanuel Macron s'est également exprimé sur les dangers de l'application.

En Italie, Matteo Salvini s'est prononcé contre l'interdiction émise par la Commission européenne.

#### Ailleurs dans le monde

À l'heure actuelle, TikTok serait tout à fait interdit (et pas seulement pour les services publics) dans plusieurs pays asiatiques, dont l'Afghanistan, l'Arménie, l'Azerbaïdjan, le Bangladesh, l'Inde, l'Iran, le

---

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

Pakistan et la Syrie. L'application aurait été temporairement interdite en Indonésie et en Jordanie, mais cette interdiction aurait depuis été levée dans ces deux pays.

Le 27 février, le **Canada** a annoncé qu'il interdisait, avec effet immédiat, l'utilisation de TikTok sur les appareils des autorités fédérales car l'application présente un risque inacceptable en matière de protection de la vie privée et de sécurité. Bien qu'il n'y ait aucune preuve que l'application ait déjà permis d'obtenir des informations publiques, les autorités ont jugé le risque trop grand. L'autorité de protection des données du Canada a également lancé une enquête, en mettant l'accent sur le traitement des données personnelles des mineurs.

Le **Royaume-Uni** est pour l'instant divisé sur la question. Le Parlement a fermé son propre compte TikTok en août 2022 et certains services publics n'utilisent plus l'application. Toutefois, la ministre des technologies, M. Donelan, s'est prononcée contre une interdiction générale de l'utilisation de TikTok par les fonctionnaires ; elle estime que cela devrait rester un choix personnel.<sup>7</sup>

### Contribution de la VSSE

Voici des extraits pertinents provenant de plusieurs réponses de la VSSE.

#### Avis de la VSSE concernant TikTok : VSSE rond TikTok:

1) *Par le passé, des experts internationaux en sécurité ont découvert que l'application TikTok présentait des vulnérabilités graves. Celles-ci ont été notamment mises en lumière par des chercheurs du bureau d'études en cybersécurité renommé Checkpoint.*

...

2) *TikTok est une plateforme de médias sociaux libre d'utilisation. Il est à noter à cet égard que le modèle de revenus de ce genre de plateformes repose souvent sur la collecte et le traitement de données à des fins commerciales. D'une part, ces données contiennent des informations relatives au contenu que les utilisateurs envoient via la plateforme. D'autre part, elles comprennent toutes les métadonnées concernant l'utilisation de l'application. Celles-ci peuvent revêtir de nombreuses formes: informations sur l'appareil et les connexions utilisées, carnet d'adresses de l'utilisateur, date et heure et données de localisation. Si l'accord de l'utilisateur est requis pour partager ce type d'informations, il s'agit souvent d'une condition essentielle pour pouvoir utiliser l'application. Dans la*

---

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

*pratique, il n'est donc pas véritablement question de choix informé pour l'utilisateur ni d'option pour mieux protéger sa vie privée. En examinant les droits d'accès demandés par l'application TikTok, on constate que ceux-ci sont très larges.*

...

*3) En tant que plateforme de médias sociaux, TikTok appartient à l'entreprise chinoise ByteDance. Cette entreprise est dès lors soumise aux règles de compliance chinoises relatives à l'accès des autorités chinoises aux données collectées par ByteDance. L'entreprise entretient de bons rapports de collaboration avec les autorités chinoises. Citons, à titre d'exemple, la disparition en Chine de Neihan Duhanzi (une plateforme de médias sociaux en Chine sur laquelle des blagues étaient partagées). TikTok n'est pas disponible en Chine et, d'après ByteDance, les données ne sont pas stockées dans ce pays. Les conditions d'utilisation de TikTok stipulent cependant bien que les données peuvent être partagées au sein du groupe. En outre, des experts (Penetrum) ont constaté que plus de 30 % des connexions de TikTok aux adresses IP allaient en Chine. Les mêmes experts affirment que les données de TikTok sont enregistrées sur des serveurs du fournisseur d'accès à internet chinois Alibaba, très proche des autorités chinoises, et que TikTok se livrerait à un traçage poussé des utilisateurs. En d'autres termes, ces utilisateurs ne peuvent pas s'attendre à la même protection de leurs données privées que dans l'Union européenne.*

*À cet égard, nous souhaitons attirer l'attention sur deux lois chinoises applicables à ByteDance, et donc également aux données collectées via TikTok..*

*Tout d'abord, la loi sur la cybersécurité, qui oblige les opérateurs de réseaux à collaborer avec les services de police et de sécurité chinois. À la demande des services de sécurité, ces entreprises sont tenues de donner intégralement accès à leurs données. Mentionnons également l'existence d'une obligation d' « assistance technique », non définie plus précisément.*

*Deuxièmement, la « loi sur le renseignement », qui régit les relations entre les services de sécurité et la société chinoise. Cette loi oblige les institutions, les organisations et les citoyens à fournir aux services de sécurité le soutien, l'assistance et la collaboration nécessaires. Par ailleurs, elle confère à ces services le droit d'accéder à tous les lieux et sources non publics « pertinents » et d'y recueillir des informations. Quels sont les éléments pertinents dans ce contexte? Il s'agit notamment de la publication ou la diffusion de messages qui mettent en péril la Sûreté de l'État et de faits fabriqués ou manipulés, d'idées pouvant être très largement interprétées par un régime qui développe une vision particulière de certains principes, tels que les droits de l'homme, la protection de la vie privée, la liberté d'expression ou encore la séparation de la justice et de l'État.*

...



S'agissant des smartphones chinois, voici l'avis de la VSSE :

*Malgré l'absence de preuves observées que les dispositifs sont utilisés à des fins d'espionnage, on peut déduire – à partir d'informations disponibles dans des sources ouvertes (en l'occurrence la législation chinoise dans le cadre de laquelle les fabricants opèrent) – qu'il est théoriquement possible que les dispositifs et les informations qu'ils traitent soient exposés à l'espionnage chinois. On recommande donc la vigilance, surtout lorsqu'il s'agit de data sensibles.*

...

*Il existe des immixtions entre ces entreprises et les autorités chinoises.*

*Cette immixtion se manifeste de plusieurs manières.*

(1) Premièrement, le Parti communiste chinois (PCC) entretient une forte emprise idéologique sur les entreprises chinoises. Ces entreprises privées doivent respecter les lignes rouges fixées par le PCC, faute de quoi elles sont privées d'accès au financement ou pénalisées d'une autre manière. En outre, le PCC dispose d'un comité au sein des entreprises de la taille de Huawei, Xiaomi, Oppo et OnePlus. Le rôle de ces cellules du parti est de veiller à ce que l'entreprise suive bien les lignes directrices du PCC ; elles peuvent influencer les décisions stratégiques des entreprises (privées).

(2) Deuxièmement, l'immixtion des autorités chinoises et de leurs services de renseignement et de sécurité est également cimentée sur le plan juridique. À titre d'exemple, nous aimerions attirer votre attention sur l'article 7 de la loi nationale chinoise sur le renseignement, qui oblige toutes les entreprises chinoises à coopérer avec les services de renseignement. L'article 24 exige des entreprises qu'elles réservent des postes au personnel des services de renseignement. La législation chinoise sur la cybersécurité de 2016, complétée en 2018, contraint par ailleurs les entreprises chinoises à octroyer aux services de renseignement un accès illimité aux systèmes informatiques. En d'autres termes, force est de constater que les entreprises n'ont d'autre choix que de coopérer avec les autorités chinoises. Il est donc question d'une ingérence systémique et approfondie.

...

*C'est pourquoi il est recommandé de ne pas installer d'applications qui ne sont pas nécessaires sur des appareils à usage professionnel, ou qui contiennent des informations sensibles. Ce conseil vaut certainement pour les applications chinoises comme TikTok.*

### Contribution du SGRS

Le SGRS a fortement déconseillé l'utilisation de TikTok au sein de la Défense pour des questions de respect de la vie privée et de sécurité. L'utilisation dans le cadre des missions de service doit faire l'objet d'une autorisation préalable, sinon elle est interdite.

Si la Défense n'impose pas d'interdiction individuelle, elle déconseille d'utiliser l'application et interdit aux unités de l'utiliser dans le cadre de leurs missions.

### Analyse technique du CCB

Il s'agit d'un dossier complexe avec de nombreux aspects et différents points de vue. Bien qu'il est difficile de savoir exactement à quelles informations TikTok a accès, les applications de médias sociaux collectent toutes un grand nombre de données personnelles, enregistrent la localisation, les contacts, les visites de sites Internet, etc. TikTok doit se conformer aux règles européennes du RGPD lors de la collecte et du traitement des données à caractère personnel. Il appartient aux autorités belges et aux autres autorités européennes de protection des données d'analyser si TikTok respecte ces exigences.

Certaines législations européennes adoptées ou proposées peuvent également contribuer au respect de ces règles. Il existe déjà le Règlement général sur la protection des données, auquel TikTok doit se conformer, et plusieurs autorités ont déjà publié des enquêtes et infligé des amendes dans ce cadre.

À partir de la mi-2023, le **Digital Services Act**<sup>8</sup> entrera également en vigueur, imposant de nouvelles règles aux opérateurs numériques en matière de modération de contenu. TikTok devra se conformer à ces règles, qui pourraient répondre à certaines préoccupations concernant l'influence et le contenu illicite.

Par ailleurs, le **Digital Markets Act**<sup>9</sup>, adopté en 2022 et qui fixe des règles concernant la concurrence des plateformes en ligne, pourrait s'appliquer à TikTok.

Le Cyber Resilience Act a été proposé en septembre 2022 et vise à imposer des exigences de sécurité à tous les produits comportant des éléments numériques, y compris les applications mobiles.

Une fois ce règlement approuvé et mis en œuvre (pas dans les deux prochaines années), TikTok devra également se conformer à ces exigences en matière de cybersécurité, ce qui pourrait se traduire par un renforcement de la sécurité.

### Le plus important dans cette analyse est toutefois l'aspect de la cybersécurité.

L'utilisation du logiciel TikTok sur les systèmes des services publics présente-t-elle un risque pour la sécurité ?

---

<sup>8</sup> [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-actensuring-safe-and-accountable-online-environment\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-actensuring-safe-and-accountable-online-environment_en)

<sup>9</sup> [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-actensuring-fair-and-open-digital-markets\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-actensuring-fair-and-open-digital-markets_en)

Pour l'heure, le CCB **ne dispose pas de rapports ou d'analyses techniques permettant d'affirmer que TikTok est fondamentalement moins sûr que d'autres applications similaires.**

Cependant, l'absence de tels rapports ou analyses techniques importe peu en général. Le risque ne réside pas tant dans le produit proprement dit que dans l'accès à l'information du producteur. Le producteur n'a donc pas besoin de vulnérabilités techniques ou de portes dérobées pour recueillir des informations.

Dans le cas des applications pour smartphones, on peut supposer que le producteur a de toute façon accès en permanence à un grand nombre d'informations personnelles de l'utilisateur. La plupart des utilisateurs de smartphones autorisent a priori les accès demandés lors de l'installation d'une nouvelle application. En outre, la **VSSE mentionne** qu'un grand nombre de connexions de l'application TikTok sont effectuées avec des adresses IP en Chine, que les données sont stockées sur les serveurs du fournisseur d'accès à Internet chinois Alibaba qui entretient de bonnes relations avec les autorités chinoises et que Tiktok se livrerait à un suivi approfondi des utilisateurs.

Les préoccupations techniques liées au partage non autorisé de données par TikTok évoqué dans les médias revêtent donc **principalement des risques de nature géopolitique**. L'identification et l'évaluation de tels risques de nature géopolitique n'est pas du ressort du CCB. En ce qui concerne les risques de sécurité liés à l'utilisation de TikTok, **le CCB suit ainsi l'avis de la Sûreté de l'État, qui est très clair.**

La meilleure solution, également mise en œuvre dans d'autres États pour faire face à ces risques géopolitiques, est de recommander de **ne pas utiliser (voire d'interdire) l'application TikTok sur les appareils de service ou les appareils accédant aux réseaux et systèmes des autorités fédérales.**

## Conclusion et avis

Un certain nombre de pays sensibilisent leur population aux risques que l'utilisation de TikTok représente pour le respect de la vie privée et interdisent son installation sur les smartphones des services publics.

Si l'utilisation de produits provenant de fournisseurs chinois est une question très complexe avec de nombreux angles et aspects différents à prendre en compte, les différents dossiers ont un point commun : les risques ne sont pas techniques mais géopolitiques.

Le CCB suit **l'avis de la VSSE en la matière : ne pas installer TikTok sur des appareils à usage professionnel.**

Bien qu'aucune vulnérabilité technique particulière ou exceptionnelle ou de porte dérobée n'ont été identifiées dans TikTok, ce n'est ici pas ce qui nous préoccupe. Le fournisseur ByteDance n'a pas

besoin de toutes ces vulnérabilités techniques pour avoir accès à un très grand nombre d'informations sensibles. De plus, TikTok stockerait des données sur des serveurs contrôlés par une entité chinoise. L'absence de rapports ou d'analyses techniques incriminantes ne change en rien les fameux risques liés à l'utilisation de TikTok.

**À la lumière de ces constatations et des informations fournies par la VSSE, voici les recommandations du CCB :**

- interdire l'utilisation de l'application TikTok sur les appareils des services fixes et mobiles

## Rapport avis TikTok

- recommander de ne pas installer ou utiliser TikTok sur des appareils personnels permettant d'accéder aux réseaux et systèmes internes des autorités fédérales
- conseiller au secteur privé de faire preuve de vigilance quant aux risques potentiels liés à l'utilisation de TikTok