

**CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE**

23 mars 2023

PROPOSITION DE LOI

**concernant l'établissement
d'une liste à l'usage de la Défense comportant
les applications et les logiciels interdits sur
les appareils de communication électronique**

(déposée par M. Theo Francken et consorts)

**BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS**

23 maart 2023

WETSVOORSTEL

**betreffende het instellen
van een lijst voor Defensie
met de verboden applicaties en software
op elektronische communicatieapparaten**

(ingediend door de heer Theo Francken c.s.)

RÉSUMÉ

Les opérations militaires et les activités quotidiennes de la Défense sont menacées par une nouvelle génération de logiciels et d'applications commerciales qui présentent un risque pour la sécurité des informations sensibles et des réseaux de communication.

Cette loi vise par conséquent à interdire l'utilisation d'applications et de logiciels qui présentent un risque potentiel pour la sécurité. L'identification de ces applications et de ces logiciels est confiée au Service Général du Renseignement et de la Sécurité (SGRS). Une fois identifiés, ils seront inscrits sur une liste régulièrement mise à jour.

Cette loi instaure une interdiction d'utilisation de ces applications et de ces logiciels tant pour le personnel de la Défense que pour le personnel du cabinet du ministre de la Défense, ainsi que pour le ministre lui-même.

Dans des cas exceptionnels, le ministre de la Défense peut autoriser le personnel de la Défense à utiliser ces applications et logiciels moyennant le respect de certaines directives et procédures.

SAMENVATTING

De militaire operaties en de dagelijkse activiteiten van Defensie worden bedreigd door een nieuwe generatie software en commerciële applicaties die een risico vormen voor de veiligheid van gevoelige informatie en de communicatienetwerken.

Daarom beoogt deze wet een verbod in te stellen op het gebruik van applicaties en software met een potentieel veiligheidsrisico. De identificatie van deze applicaties en software gebeurt door de Algemene Dienst Inlichting en Veiligheid (ADIV), waarna deze opgenomen worden op een lijst die op regelmatige basis wordt bijgewerkt.

Deze wet voert een verbod tot gebruik van deze applicaties en software in voor zowel het personeel van Defensie, voor het personeel van het kabinet van de minister van Landsverdediging als voor de minister van Landsverdediging zelf.

In uitzonderlijke gevallen kan de minister van Landsverdediging aan het personeel van Defensie toelating geven tot het gebruik van deze applicaties en software mits het naleven van bepaalde richtlijnen en procedures.

N-VA	: Nieuw-Vlaamse Alliantie
Ecolo-Groen	: Ecologistes Confédérés pour l'organisation de luttes originales – Groen
PS	: Parti Socialiste
VB	: Vlaams Belang
MR	: Mouvement Réformateur
cd&v	: Christen-Democratisch en Vlaams
PVDA-PTB	: Partij van de Arbeid van België – Parti du Travail de Belgique
Open Vld	: Open Vlaamse liberalen en democraten
Vooruit	: Vooruit
Les Engagés	: Les Engagés
DéFI	: Démocrate Fédéraliste Indépendant
INDEP-ONAFH	: Indépendant – Onafhankelijk

Abréviations dans la numérotation des publications:		Afkorting bij de nummering van de publicaties:	
DOC 55 0000/000	Document de la 55 ^e législature, suivi du numéro de base et numéro de suivi	DOC 55 0000/000	Parlementair document van de 55 ^e zittingsperiode + basisnummer en volgnummer
QRVA	Questions et Réponses écrites	QRVA	Schriftelijke Vragen en Antwoorden
CRIV	Version provisoire du Compte Rendu Intégral	CRIV	Voorlopige versie van het Integraal Verslag
CRABV	Compte Rendu Analytique	CRABV	Beknopt Verslag
CRIV	Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)	CRIV	Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)
PLEN	Séance plénière	PLEN	Plenum
COM	Réunion de commission	COM	Commissievergadering
MOT	Motions déposées en conclusion d'interpellations (papier beige)	MOT	Moties tot besluit van interpellaties (beigegekleurig papier)

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

La confidentialité et la protection des informations sont des éléments essentiels de la culture militaire depuis des siècles. Pour garantir cette confidentialité et assurer cette protection, des sanctions strictes ont depuis toujours été appliquées à la diffusion non autorisée d'informations classifiées et opérationnelles, que ce soit à l'intérieur ou à l'extérieur de la Défense. L'organisation est en effet exposée à toutes sortes d'activités de renseignement (ROHUM¹, ROEM² et leurs sous-disciplines, en nombre croissant) menées par des acteurs étrangers qui s'intéressent à elle.

En ce 21^e siècle, les opérations militaires et les activités quotidiennes de la Défense sont menacées par une nouvelle génération de logiciels et d'applications commerciales qui présentent un risque pour la sécurité des informations sensibles et des réseaux de communication de l'organisation.

Ces logiciels et ces applications commerciales peuvent accéder aux données captées par le microphone ou la caméra d'un appareil, aux données de localisation, aux listes de contacts, aux recherches effectuées et à d'autres informations numériques. Ces données peuvent être utilisées pour analyser le comportement des utilisateurs, traiter ces données et les partager avec l'éditeur. Ces données peuvent également être instrumentalisées afin de répandre discrètement et de manière ciblée de fausses informations et de la propagande parmi le personnel militaire.

Un exemple de ce type d'application est la plateforme du réseau social populaire TikTok, qui est détenue par la société chinoise ByteDance et qui est de plus en plus souvent considérée comme un risque potentiel pour la sécurité. Ce réseau social est souvent cité comme exemple d'ingérence probable de la part d'un acteur étatique étranger, ce qui a conduit certains pays alliés, dont les États-Unis, à en interdire l'utilisation à leur personnel militaire.

À heure actuelle, une telle culture de la sécurité n'existe pas encore en Belgique vis-à-vis du danger croissant lié à la collecte de données. S'il existe bien des directives internes visant à restreindre l'utilisation d'applications personnelles en fonction du niveau de menace de la

¹ Renseignement d'origine humaine (en anglais: *Human intelligence* ou HUMINT).

² Renseignement d'origine électromagnétique (en anglais: *Signals intelligence* ou SIGINT).

TOELICHTING

DAMES EN HEREN,

De vertrouwelijkheid en het beschermen van informatie zijn al eeuwenlang cruciale onderdelen van de militaire cultuur. Om dit te waarborgen worden er van oudsher strikte sancties toegepast op de ongeoorloofde verspreiding van geclassificeerde en operationele informatie binnen en buiten Defensie. De organisatie staat immers bloot aan velerlei vormen van HUMINT¹ en SIGINT² en hun groeiend aantal subdisciplines door buitenlandse actoren die er belang bij hebben om haar te schaduwen.

In de 21^e eeuw worden de militaire operaties en de dagelijkse activiteiten van Defensie echter bedreigd door een nieuwe generatie software en commerciële applicaties die een risico vormen voor de veiligheid van gevoelige informatie en de communicatienetwerken van Defensie.

Deze software en commerciële applicaties kunnen zich toegang verschaffen tot de microfoon-, camera- en locatiegegevens, contactenlijsten, zoekopdrachten en andere digitale informatie. Deze gegevens kunnen worden gebruikt om het gedrag van hun gebruikers te analyseren, te verwerken en te delen met de uitgever. Daarnaast kunnen ze geïnstrumentaliseerd worden om gericht en onbewust nepnieuws en propaganda onder het militair personeel te verspreiden.

Een voorbeeld van een dergelijke applicatie is het populaire socialenetwerkplatform TikTok, dat eigendom is van het Chinese ByteDance en dat steeds vaker als potentieel veiligheidsrisico wordt genoemd. Het is een vaak genoemd voorbeeld van vermoedelijke inmenging door een buitenlandse statelijke actor, wat sommige geallieerde overheden, waaronder de Verenigde Staten, een verbod heeft laten instellen op het gebruik door hun militair personeel.

In België ontbreekt op dit moment nog een vergelijkbare veiligheidscultuur met betrekking tot het groeiende gevaar van datacollectie. Hoewel er interne richtlijnen worden opgelegd voor het gebruik van persoonlijke applicaties op basis van het dreigingsniveau van de regio

¹ HUMINT is *Human Intelligence*.

² SIGINT is *intelligence derived from electronic signals and systems used by foreign targets (such as communication systems, radars and weapon systems)*.

région où des militaires sont déployés, il n'y a en revanche pas d'interdiction légale explicite, pour le personnel de la Défense, d'utiliser des applications commerciales spécifiques tant qu'il n'y a pas de communication déli-
bérée d'informations classifiées.

C'est pourquoi il est nécessaire d'interdire l'utilisation d'applications et de logiciels qui présentent un risque potentiel pour la sécurité. Nous chargeons le Service Général du Renseignement et de la Sécurité (SGRS) d'identifier ces applications et ces logiciels, après quoi ils seront inscrits sur une liste qui sera régulièrement mise à jour.

Cette interdiction devra s'appliquer à tout moment à tout appareil de communication électronique (comme les téléphones et les tablettes) à usage professionnel fourni par la Défense, ainsi qu'à tous les appareils de communication électronique personnels, qu'ils soient utilisés sur des sites appartenant à la Défense ou lors de formations externes, d'entraînements ou d'opérations sur le terrain. Il sera également interdit d'utiliser ces applications et ces logiciels sur des appareils de communication électronique personnels sur lesquels ont également été installés des applications ou des logiciels édités par la Défense ou destinés à l'exercice d'une fonction en son sein.

D'autre part, l'interdiction concerne également le ministre lui-même et son cabinet, compte tenu des liens étroits et du partage intense d'informations (y compris de données sensibles) entre le ministre de la Défense, les organes politiques ministériels et le département de la Défense.

Pour assurer la sécurité des informations sensibles et des réseaux de communication, il est essentiel que cette interdiction soit respectée et que le personnel de la Défense soit conscient des risques liés à l'utilisation d'applications et de logiciels qui présentent un risque potentiel pour la sécurité. Pour y parvenir, il convient de former et de sensibiliser régulièrement le personnel à l'importance de la sécurisation de l'information et aux dangers que pose l'utilisation d'applications et de logiciels peu sûrs.

waar militairen worden ingezet, is er geen uitdrukkelijk wettelijk verbod voor het personeel van Defensie om specifieke commerciële applicaties te gebruiken, zolang er geen bewuste communicatie van geclassificeerde informatie plaatsvindt.

Daarom is het nodig om een verbod in te stellen op het gebruik van applicaties en software met een potentieel veiligheidsrisico. Dit wetsvoorstel legt de taak voor de identificatie van deze applicaties en software bij de Algemene Dienst Inlichting en Veiligheid (ADIV), waarna deze opgenomen worden op een lijst die op regelmatige basis wordt bijgewerkt.

Dit verbod moet te allen tijde gelden voor elk elektronische communicatieapparaat (zoals telefoons en tablets) voor professioneel gebruik, verstrekt door Defensie en voor alle persoonlijke elektronische communicatieapparaten die worden gebruikt binnen de eigendommen van Defensie, tijdens externe opleidingen, trainingen of operaties. Maar ook om deze te gebruiken op het persoonlijke elektronische toestel waarop ook software of applicaties staan, uitgegeven of bestemd door Defensie voor de uitoefening van de functie

Het verbod betreft anderzijds ook de minister zelf en zijn of haar kabinet, gelet de innige band en informatie-
deling op hoog niveau tussen de functie van de minister van Landsverdediging, de ministeriële beleidsorganen en Defensie waarbij gevoelige data worden gedeeld.

Om de veiligheid van gevoelige informatie en communicatienetwerken te waarborgen, is het essentieel dat dit verbod wordt nageleefd en dat het personeel van Defensie zich bewust is van de risico's van het gebruik van applicaties en software met een potentieel veiligheidsrisico. Dit kan worden bereikt door regelmatige training en bewustmaking van het personeel over het belang van informatiebeveiliging en de gevaren van onveilige applicaties en software.

Theo Francken (N-VA)
Michael Freilich (N-VA)
Peter Buysrogge (N-VA)
Darya Safai (N-VA)
Frieda Gijbels (N-VA)
Kristien Van Vaerenbergh (N-VA)
Kathleen Depoorter (N-VA)
Sigrid Goethals (N-VA)

PROPOSITION DE LOI**Article 1^{er}**

La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2

Une liste des logiciels et des applications présentant un risque potentiel en cas d'utilisation par des membres du personnel de la Défense dans l'exercice de leurs fonctions est établie annuellement par le Service Général du Renseignement et de la Sécurité (SGRS). Cette liste, après approbation par le Conseil des ministres, est annexée à la présente loi.

Art. 3

Afin d'identifier d'éventuels dangers potentiels, le Service Général du Renseignement et de la Sécurité (SGRS) procède chaque année à une analyse des logiciels et des applications commerciales les plus couramment utilisés sur les appareils de communication mis à disposition par la Défense.

Art. 4

Il est interdit aux membres du personnel de la Défense d'installer ou d'utiliser sur leurs appareils de communication électronique professionnels des logiciels ou des applications figurant sur la liste visée à l'article 2.

Art. 5

Il est interdit aux membres du personnel de la Défense d'utiliser sur leurs appareils de communication électronique personnels des logiciels ou des applications figurant sur la liste visée à l'article 2 s'ils sont utilisés à l'intérieur du périmètre de sites appartenant à la Défense ou lors de formations externes, de missions d'entraînement ou d'opérations sur le terrain.

Art. 6

Il est interdit aux membres personnel de la Défense d'installer ou d'utiliser sur leurs appareils de communication électronique personnels des logiciels ou des applications figurant sur la liste visée à l'article 2 en

WETSVOORSTEL**Artikel 1**

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

Een lijst van software en applicaties, die een potentiële risico inhouden voor het gebruik door het personeel van Defensie tijdens de uitoefening van hun functie, wordt jaarlijks opgemaakt door de Algemene Dienst Inlichting en Veiligheid (ADIV) en, na de goedkeuring door de Ministerraad, als bijlage bij deze wet gevoegd.

Art. 3

Om potentiële gevaren te identificeren voert de Algemene Dienst Inlichting en Veiligheid (ADIV) jaarlijks een doorlichting door van de meest gebruikte commerciële software en applicaties op de door Defensie verstrekte communicatieapparaten.

Art. 4

Voor het personeel van Defensie is het verboden om software of applicaties, vermeld op de lijst als bedoeld in artikel 2, te installeren of te gebruiken op hun professionele elektronische communicatietoestellen.

Art. 5

Voor het personeel van Defensie is het verboden om software of applicaties, vermeld op de lijst als bedoeld in artikel 2, te gebruiken op hun persoonlijke elektronische communicatietoestellen indien die worden gebruikt binnen de perimeter van eigendommen van Defensie, tijdens externe opleidingen, trainingsopdrachten of operaties.

Art. 6

Voor het personeel van Defensie is het verboden om software of applicaties, vermeld op de lijst als bedoeld in artikel 2, te installeren of te gebruiken op hun persoonlijke elektronische communicatietoestellen in combinatie

combinaison avec des applications ou des logiciels édités par la Défense ou destinés à l'exercice de leur profession.

Art. 7

Il est interdit aux membres du personnel appartenant au cabinet du ministre ayant la Défense nationale dans ses attributions d'installer ou d'utiliser sur leurs appareils de communication électronique professionnels des logiciels ou des applications figurant sur la liste visée à l'article 2.

Art. 8

Il est interdit aux membres du personnel qui font partie du cabinet du ministre ayant la Défense nationale dans ses attributions d'installer ou d'utiliser sur leurs appareils de communication électronique professionnels des logiciels ou des applications figurant sur la liste visée à l'article 2 à l'intérieur du périmètre de sites appartenant à la Défense ou en combinaison avec des applications ou des logiciels édités par la Défense ou destinés à l'exercice d'une profession en son sein.

Art. 9

Il est interdit au ministre ayant la Défense nationale dans ses attributions d'installer ou d'utiliser sur ses appareils de communication électronique professionnels des logiciels ou des applications figurant sur la liste visée à l'article 2.

Art. 10

Il est interdit au ministre ayant la Défense nationale dans ses attributions d'installer ou d'utiliser sur ses appareils de communication électronique professionnels des logiciels ou des applications figurant sur la liste visée à l'article 2 à l'intérieur du périmètre de sites appartenant à la Défense ou en combinaison avec des applications ou des logiciels édités par la Défense ou destinés à l'exercice d'une profession en son sein.

Art. 11

Le ministre ayant la Défense nationale dans ses attributions est chargé de faire respecter les interdictions visées aux articles 4 à 10 de la présente loi et d'élaborer les directives et procédures nécessaires à son application.

met software of applicatie uitgegeven of bestemd door Defensie voor de uitoefening van het beroep.

Art. 7

Voor de personeelsleden die deel uitmaken van het kabinet van de minister bevoegd voor de Landsverdediging, is het verboden om software of applicaties, vermeld op de lijst als bedoeld in artikel 2, te installeren of te gebruiken op hun professionele elektronische communicatietoestellen.

Art. 8

Voor de personeelsleden die deel uitmaken van het kabinet van de minister bevoegd voor de Landsverdediging, is het verboden om software of applicaties, vermeld op de lijst als bedoeld in artikel 2, te installeren of te gebruiken op hun persoonlijke elektronische communicatietoestellen binnen de perimeter van eigendommen van Defensie of in combinatie met software of applicatie uitgegeven of bestemd door Defensie voor de uitoefening van het beroep.

Art. 9

Voor de minister bevoegd voor de Landsverdediging is het verboden om software of applicaties, vermeld op de lijst als bedoeld in artikel 2, te installeren of te gebruiken op zijn professionele elektronische communicatietoestellen.

Art. 10

Voor de minister bevoegd voor de Landsverdediging, is het verboden om software of applicaties, vermeld op de lijst als bedoeld in artikel 2, te installeren of te gebruiken op zijn persoonlijke elektronische communicatietoestellen binnen de perimeter van eigendommen van Defensie of in combinatie met software of applicatie uitgegeven of bestemd door Defensie voor de uitoefening van het beroep.

Art. 11

De minister bevoegd voor de Landsverdediging is verantwoordelijk voor het handhaven van de verboden zoals bedoeld in de artikelen 4 tot 10 van deze wet en voor het opstellen van nodige richtlijnen en procedures ter uitvoering van deze wet.

Art. 12

Dans des cas exceptionnels, lorsque l'utilisation de logiciels ou d'applications figurant sur la liste visée à l'article 2 est nécessaire à des fins officielles, le ministre ayant la Défense nationale dans ses attributions peut autoriser le personnel de la Défense à les utiliser sur des appareils de communication électronique professionnels ou personnels.

Art. 13

Les membres du personnel de la Défense ayant obtenu l'autorisation, visée à l'article 12, d'utiliser une application ou un logiciel interdit à des fins officielles doivent respecter strictement les directives et les procédures visant une utilisation sûre établies, conformément à l'article 11, par le ministre ayant la Défense nationale dans ses attributions.

Art. 14

Des mesures disciplinaires peuvent être prises à l'encontre du personnel de la Défense qui ne respecterait pas les interdictions visées aux articles 4 à 8 ou les directives et procédures visées à l'article 11, et ce, conformément à la loi du 14 janvier 1975 portant le règlement de discipline des Forces armées.

Art. 15

Le ministre ayant la Défense nationale dans ses attributions doit informer en temps utile le personnel de la Défense des modifications apportées à la liste visée à l'article 2 et prévoir pour le personnel des formations et des actions de sensibilisation régulières sur les dangers posés par l'utilisation d'applications et de logiciels peu sûrs.

Art. 16

La présente loi entre en vigueur le jour de sa publication au *Moniteur belge*.

Art. 12

In uitzonderlijke gevallen, wanneer het gebruik van software of applicaties vermeld op de lijst als bedoeld in artikel 2, noodzakelijk is voor officiële doeleinden, kan de minister bevoegd voor de Landsverdediging aan het personeel van Defensie toestemming geven tot het gebruik van de applicatie op professionele toestellen of persoonlijke toestellen.

Art. 13

Het personeel van Defensie dat de toestemming, als bedoeld in artikel 12, heeft gekregen voor het gebruik voor officiële doeleinden, moet zich strikt houden aan de richtlijnen en procedures voor veilig gebruik zoals opgesteld door de minister bevoegd voor de Landsverdediging conform artikel 11.

Art. 14

Aan het personeel van Defensie dat zich niet houdt aan de verboden als bedoeld in de artikelen 4 tot 8 of aan de richtlijnen en procedures als bedoeld in artikel 11, kunnen tuchtmaatregelen worden opgelegd conform de wet van 14 januari 1975 houdende het tuchtreglement van de Krijgsmacht.

Art. 15

De minister bevoegd voor de Landsverdediging moet het personeel van Defensie tijdig in kennis stellen van de wijzigingen aan de lijst als bedoeld in artikel 2 en voorzien in regelmatige trainingen en een bewustmaking van het personeel over de gevaren van onveilige applicaties en software.

Art. 16

Deze wet treedt in werking de dag waarop ze in het *Belgisch Staatsblad* wordt bekendgemaakt.

Theo Francken (N-VA)
Michael Freilich (N-VA)
Peter Buysrogge (N-VA)
Darya Safai (N-VA)
Frieda Gijbels (N-VA)
Kristien Van Vaerenbergh (N-VA)
Kathleen Depoorter (N-VA)
Sigrid Goethals (N-VA)