DOC 56 **0322/001**

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

8 oktober 2024

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.)

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

8 octobre 2024

PROPOSITION DE LOI

concernant l'établissement d'une liste, à l'usage de la Défense, des applications et des logiciels dont l'installation et l'utilisation sont interdites sur certains appareils de communication électronique

(déposée par M. Theo Francken et consorts)

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.

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.

00367

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

Abréviations dans la numérotation des publications:		*Afkorting bij de nummering van de publicaties:*	
DOC 56 0000/000	*Document de la 56e législature, suivi du numéro de base et numéro de suivi*	*DOC 56 0000/000*	*Parlementair document van de 56e 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 (beigekleurig papier)*

TOELICHTING

DAMES EN HEREN,

Dit voorstel neemt, met een aantal aanpassingen, de tekst over van voorstel DOC 55 3254/001.

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 HUMINT[1] en SIGINT[2] en hun groeiend aantal subdisciplines door buitenlandse actoren die er belang bij hebben om haar te schaduwen.

In de 21e 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

[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).*

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

La présente proposition reprend, en l'adaptant, le texte de la proposition DOC 55 3254/001.

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 (ROHUM[1], ROEM[2] et leurs sous-disciplines, en nombre croissant) menées par des acteurs étrangers qui s'intéressent à elle.

En ce 21e 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

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

[2] Renseignement d'origine électromagnétique (en anglais: S*ignals intelligence* ou SIGINT).

gevaar van datacollectie. Hoewel er interne richtlijnen worden opgelegd voor het gebruik van persoonlijke applicaties op basis van het dreigingsniveau van de regio 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 informatiedeling 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)

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 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 délibérée 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.

WETSVOORSTEL

Artikel 1

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

Art. 2

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

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

Art. 3

Het is verboden voor Defensiepersoneel om software of applicaties, vermeld op deze lijst, te installeren of te gebruiken:

1° op hun professionele elektronische communicatietoestellen;

2° op hun persoonlijke elektronische communicatietoestellen, die worden gebruikt binnen de perimeter van de militaire domeinen, tijdens externe opleidingen of trainingsopdrachten, of in operaties;

3° op hun persoonlijke elektronische communicatietoestellen in combinatie met software of applicaties uitgegeven of bestemd door Defensie voor de uitoefening van het beroep.

Art. 4

Het is verboden voor personeelsleden die deel uitmaken van het kabinet van de minister bevoegd voor Landsverdediging, om software of applicaties, vermeld op deze lijst, te installeren of te gebruiken:

1° op hun professionele elektronische communicatietoestellen;

PROPOSITION DE LOI

Article 1er

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

Art. 2

§ 1er. La 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). Après son approbation par le Conseil des ministres, cette liste est annexée à la présente loi.

§ 2. Pour identifier d'éventuels dangers potentiels, le SGRS analyse chaque année les logiciels et les applications commerciales les plus couramment utilisés sur les appareils de communication mis à disposition par la Défense.

Art. 3

Il est interdit aux membres du personnel de la Défense d'installer ou d'utiliser les logiciels ou les applications inscrits sur cette liste:

1° sur leurs appareils de communication électronique professionnels;

2° sur leurs appareils de communication électronique personnels s'ils sont utilisés à l'intérieur du périmètre des domaines militaires, lors de formations externes, de missions d'entraînement ou d'opérations sur le terrain;

3° sur leurs appareils de communication électronique personnels en combinaison avec des logiciels ou des applications édités par la Défense ou destinés à l'exercice de leur profession.

Art. 4

Il est interdit aux membres du personnel du cabinet du ministre qui a la Défense nationale dans ses attributions d'installer ou d'utiliser des logiciels ou des applications inscrits sur cette liste:

1° sur leurs appareils de communication électronique professionnels;

2° op hun persoonlijke elektronische communicatietoestellen binnen de perimeter van de militaire domeinen;

3° op hun persoonlijke elektronische communicatietoestellen in combinatie met software of applicaties uitgegeven of bestemd door Defensie voor de uitoefening van het beroep.

Art. 5

Het is verboden voor de minister bevoegd voor Landsverdediging om software of applicaties, vermeld op deze lijst, te installeren of te gebruiken

1° op zijn of haar professionele elektronische communicatietoestellen;

2° op zijn of haar persoonlijke elektronische communicatietoestellen binnen de perimeter van de militaire domeinen;

3° op zijn of haar persoonlijke elektronische communicatietoestellen in combinatie met software of applicaties uitgegeven of bestemd door Defensie voor de uitoefening van het beroep.

Art. 6

§ 1. De minister bevoegd voor Landsverdediging handhaaft dit verbod en stelt daartoe de nodige richtlijnen en procedures op.

§ 2. In uitzonderlijke gevallen wanneer het gebruik van software of applicaties, vermeld op de voorgaand genoemde lijst, nodig is voor officiële doeleinden, kan de minister bevoegd voor Landsverdediging aan het Defensiepersoneel toestemming verlenen voor het gebruik van de applicaties op professionele toestellen of persoonlijke toestellen.

§ 3. Het Defensiepersoneel dat de toestemming, vermeld in paragraaf 2, heeft gekregen voor het gebruik voor officiële doeleinden moet zich, voor veilig gebruik, strikt houden aan de richtlijnen en procedures opgesteld door de minister bevoegd voor Landsverdediging.

Art. 7

Aan het Defensiepersoneel dat zich niet houdt aan het verbod zoals bedoeld in artikel 3 of aan de richtlijnen en procedures zoals bedoeld in artikel 6, § 3, kunnen tuchtmaatregelen worden opgelegd, conform de wet

2° sur leurs appareils de communication électronique personnels s'ils sont utilisés à l'intérieur du périmètre des domaines militaires;

3° sur leurs appareils de communication électronique personnels en combinaison avec des logiciels ou des applications édités par la Défense ou destinés à l'exercice de leur profession.

Art. 5

Il est interdit au ministre qui a la Défense nationale dans ses attributions d'installer ou d'utiliser des logiciels ou des applications figurant sur cette liste:

1° sur ses appareils de communication électronique professionnels;

2° sur ses appareils de communication électronique personnels s'ils sont utilisés à l'intérieur du périmètre des domaines militaires;

3° sur ses appareils de communication électronique personnels en combinaison avec des logiciels ou des applications édités par la Défense ou destinés à l'exercice d'une profession en son sein.

Art. 6

§ 1er. Le ministre qui a la Défense nationale dans ses attributions veille au respect de ces interdictions et élabore les directives et les procédures nécessaires à cette fin.

§ 2. Dans certains cas exceptionnels, si l'utilisation de logiciels ou d'applications inscrits sur la liste précitée est nécessaire à des fins officielles, le ministre qui a 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.

§ 3. Les membres du personnel de la Défense ayant obtenu l'autorisation visée au § 2 pour des fins officielles doivent se conformer strictement, en vue d'une utilisation sûre, aux directives et aux procédures établies par le ministre qui a la Défense nationale dans ses attributions.

Art. 7

Conformément à la loi du 14 janvier 1975 portant le règlement de discipline des Forces armées, des mesures disciplinaires peuvent être prises à l'encontre de tout membre du personnel de la Défense qui ne se conforme

van 14 januari 1975 houdende het tuchtreglement van de Krijgsmacht.

Art. 8

De minister bevoegd voor Landsverdediging stelt het Defensiepersoneel tijdig in kennis van de wijzigingen aan de lijst, zoals bedoeld in artikel.2, § 1, en voorziet in de regelmatige training en bewustmaking van het personeel over de gevaren van onveilige applicaties en software.

30 september 2024

Theo Francken (N-VA)
Michael Freilich (N-VA)
Peter Buysrogge (N-VA)
Darya Safai (N-VA)

pas à l'interdiction visée à l'article 3 ou aux directives et aux procédures visées à l'article 6, § 3.

Art. 8

Le ministre qui a la Défense nationale dans ses attributions informe le personnel de la Défense des modifications apportées à la liste visée à l'article 2, § 1er, en temps utile, et prévoit, pour le personnel, des formations et des actions de sensibilisation régulières sur les risques liés à l'utilisation d'applications et de logiciels peu sûrs.

30 septembre 2024

Centrale drukkerij - Imprimerie centrale