



Antwoord op de parlementaire vraag nr. 1595 van 16 augustus 2016 van de Heer DESEYN Roel, Volksvertegenwoordiger.

Réponse à la question parlementaire n° 1595 du 16 août 2016 de Monsieur DESEYN Roel, Député.

Betreft: Internetcensuur

1-2.

Het blokkeren van websites op last van een magistraat is enkel mogelijk in het kader van een gerechtelijke procedure. Vragen die betrekking hebben op de blokkering van websites in deze context behoren tot de bevoegdheid van mijn collega, de minister van Justitie.

Ik kan u wel informeren over de werkwijze van de IRU – Internet Referral Unit. Deze cel binnen DJSOC speurt actief het internet af om extremistische propaganda en illegale inhoud te detecteren en deze (vrijwillig te) laten verwijderen in samenwerking met de service providers.

Via een Europese gecoördineerde aanpak proberen de lidstaten de grote service providers te bewegen tot een betere samenwerking. Bepaalde grote spelers zijn zeer medewerkend en nemen zelf initiatieven om hun platformen maximaal te beschermen tegen misbruik door extremistische en terroristische groeperingen.

Zo hebben de meeste onder hen

Objet: Censure Internet

1-2.

Le blocage de sites web sur les ordres d'un magistrat est uniquement possible dans le cadre d'une procédure judiciaire. Les questions relatives au blocage de sites dans ce contexte relèvent de la compétence de mon collègue, le ministre de la Justice.

Je peux néanmoins vous informer au sujet du fonctionnement de l'IRU – Internet Referral Unit. Cette cellule, qui fait partie de la DJSOC, a pour mission de passer Internet au peigne fin en vue de détecter la propagande extrémiste et le contenu illégal et de procéder (volontairement) à leur retrait en collaboration avec les fournisseurs de services.

Grâce à une approche européenne coordonnée, les Etats Membres tentent d'encourager les « grands » providers de services « *Over the Top – OTT* » à mieux collaborer.

Certains grands FSI sont très coopératifs et prennent des initiatives pour protéger au mieux leurs plateformes contre les abus de groupes terroristes et extrémistes.

Ainsi, la plupart d'entre eux disposent

zogenaamde "trusted flagger programmes"; meldingen die door deze personen gemaakt worden sneller behandeld omdat ze meer garantie geven dat ze effectief inhoud aangeven die indruist tegen de gebruiksvoorwaarden.

De IRU heeft de "trusted flagger"-status aangevraagd aan verschillende socialemediaplatformen. Ook de nieuwe "hash-databank" die de referenties van gekende beelden van extremistische en terroristische propaganda opslaat zodat de aangesloten platformen beeldmateriaal dat gepost wordt automatisch kunnen aftoetsen aan de opgeslagen beelden en zo zonder menselijke tussenkomst het opladen van bepaalde beelden kunnen verhinderen, is een nieuw initiatief van onder meer Twitter, Facebook en YouTube.

Er moet ook aandacht worden besteed aan de kleine platformen en nieuwkomers die ontwikkeld zouden kunnen worden en zich richten op het niet-gereguleerde niveau naar aanleiding van de aanpassing aan de normen door de grote ISP, en op die manier proberen om een bepaald cliënteel terug te winnen.

De eerste stap zal zijn om de nieuwe beelden manueel op te sporen en te identificeren (hetgeen een menselijke tussenkomst impliceert) om op die manier de eventuele fout-positieve bepalingen op te sporen en de rechten van de internetgebruikers zoveel mogelijk te beveiligen.

Een tweede stap zal zijn om deze firma's ervan te overtuigen zich aan te sluiten bij het programma, dat ertoe strekt de publicatie en verspreiding van dit type inhoud te beperken.

3-4.

De afdeling DJSOC/i2_BE-IRU werd begin 2016 opgericht. Ik beschik

de "trusted flagger programmes" qui permettent un traitement plus rapide des signalements effectués par des personnes fournissant davantage de garanties que le contenu signalé va effectivement à l'encontre des conditions d'utilisation.

L'IRU a demandé le statut "trusted flagger" à différentes plates-formes de médias sociaux. Citons également la nouvelle initiative de Twitter, Facebook et YouTube entre autres, à savoir la "hash-database" qui enregistre les références d'images connues de propagande extrémiste et terroriste pour que les plates-formes connectées puissent automatiquement confronter les images postées aux images enregistrées et empêcher ainsi, sans intervention humaine donc, le chargement de certaines images.

Il convient également de porter une attention aux petites plates-formes et nouveaux venus qui pourraient se développer et s'orienter vers le niveau non réglementé suite à la mise aux normes par les grands FSI, et ainsi tenter de récupérer une certaine clientèle.

La première étape sera de détecter et d'identifier manuellement les nouvelles images (ce qui implique une intervention humaine) pour détecter de la sorte les éventuels faux positifs et sécuriser au maximum les droits des internautes.

Une seconde étape sera de convaincre ces sociétés de se joindre au programme tendant à limiter la publication et la diffusion de ce type de contenu.

3- 4.

Le service DJSOC/i2-IRU a été créé début 2016. Dès lors, je ne possède

derhalve over geen cijfer voor de vorige jaren.

Sinds de oprichting van DJSOC/i2 en de cel BE-IRU zijn 520 interventies én vragen tot blokkering van de inhoud door de afdeling behandeld.

Verdeling:

Facebook	261
Twitter	156
Google +	55
You Tube	30
FileHoster	2
Blogs	4
Site Web	8
Telegram	1
Archives.org	2
VideoPress	1

Hier valt zeker op te merken dat, in het kader van de aanslagen in Brussel en Zaventem, DJSOC/i2-IRU 269 interventies en aanvragen tot blokkering heeft behandeld. Het merendeel van de betrokken ISP's heeft snel gereageerd door over te gaan tot de gevraagde blokkeringen, voornamelijk inhoud op sociale media platformen.

De IRU nam eveneens deel aan de tweedaagse Europol IRU Action Days eind november, waarop onze Belgische onderzoeker samen met zijn 7 collega's uit Nederland, Frankrijk, Roemenië en Europol niet minder dan 1800 haatzaaiende, extremistische sites of accounts detecteerden en om hun verwijdering vroegen.

Zoals reeds vermeld worden de profielen of websites waarvan hier sprake niet door de gerechtelijke overheid geblokkeerd. De providers hebben zelf deze websites afgesloten: na contactname hebben ze hun TOS (Terms of Services: de gebruiksvoorwaarden van het platform bepaald door de providers, toegangsleveranciers, ...) strikt toegepast. De sluitingsaanvragen

pas de chiffres pour les années antérieures.

Depuis la mise en place de DJSOC/i2 et de la cellule BE-IRU, 520 interventions et demandes de blocage de contenus ont été traitées par la section i2.

Répartition:

Facebook	261
Twitter	156
Google +	55
You Tube	30
FileHoster	2
Blogs	4
Site Web	8
Telegram	1
Archives.org	2
VideoPress	1

Il faut toutefois signaler que, dans le cadre des attentats de Bruxelles et de Zaventem, DJSOC/i2-IRU a été amenée à traiter 269 interventions et demandes de blocage. La plupart des FSI concernés ont réagi rapidement en procédant aux retraits demandés, lesquels concernaient essentiellement le contenu de plates-formes de réseaux sociaux.

Fin novembre, l'IRU a également participé aux IRU Action Days d'Europol, deux jours durant lesquels notre chercheur belge et sept autres collègues des Pays-Bas, de France, de Roumanie et d'Europol ont détecté et demandé le retrait de pas moins de 1800 sites ou comptes extrémistes et haineux.

Comme déjà mentionné, les profils ou sites web dont question n'ont pas été bloqués par les autorités judiciaires. Les fournisseurs eux-mêmes ont fermé ces sites : suite à une prise de contact, ceux-ci ont appliqué de façon stricte leurs TOS (Terms of Services : les conditions d'utilisation de la plateforme définies par les providers, fournisseurs d'accès, ...). Les demandes de fermeture se sont basées

gebeurden op basis van de inhoud van de websites, namelijk radicaliserende inhoud, terroristische of gewelddadige propaganda of extremisme.

Wanneer een website/profiel verwijderd wordt, moet de houder rechtstreeks contact opnemen met de desbetreffende service provider die dan zal beslissen.

5. De Fax was het communicatiemiddel dat vroeger standaard werd gebruikt om te communiceren met de internetproviders.

Meer en meer wensten de internetproviders de aanvragen op een digitale manier te verkrijgen.

De diensten van DJSOC proberen dan om het gebruik van de Fax te rationaliseren. Het voordeel van deze tool blijft dat hij het mogelijk maakt om spam en andere gewenste e-mails te voorkomen.

sur le contenu des sites, à savoir du contenu radicalisant, de la propagande terroriste, violente ou extrémiste.

Quand un site web/profil est retiré, le détenteur doit prendre directement contact avec le fournisseur concerné qui tranchera.

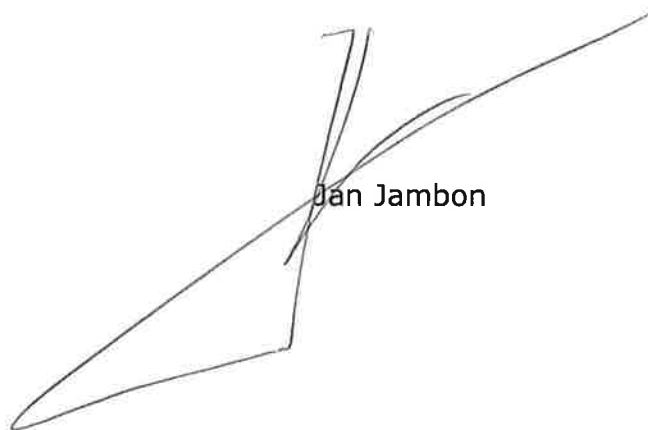
5. Le Fax était le moyen de communication utilisé auparavant par défaut pour communiquer avec les fournisseurs d'accès.

De plus en plus, ces fournisseurs d'accès souhaitent obtenir les demandes par voie électronique.

Les services de la DJSOC tendent donc de rationaliser l'utilisation du mode « Fax ». L'avantage de cet outil reste qu'il permet d'éviter les spams et autres mails indésirables.

De Minister,

Le Ministre,



Jan Jambon