Lettre n°71 – Février 2018 - disponible sur omc.ceis.eu

TABLE DES MATIERES

DES ENJEUX DE L'APPLICATION DU RGPD

Le 25 mai prochain, tous les organismes européens, tant publics que privés, qui traitent des données personnelles de personnes se trouvant sur le territoire de l'Union devront appliquer le nouveau règlement général européen sur la protection des données (RGPD).

En effet, abrogeant la directive européenne 96/46/CE, le RGPD (Règlement UE 2016/679[1]) est désormais le texte de référence européen en matière de protection des données personnelles et de libre circulation de ces données. Adopté le 27 avril 2016 après quatre longues années de travail et de négociations, ce texte sera directement applicable dans l'ensemble de l'Union européenne (UE) sans nécessiter de transposition en droit interne par les États membres[2].

Les objectifs et les apports du RGPD

Cette réforme globale du cadre européen de protection des données personnelles marque un tournant dans la régulation des données personnelles[3]. Elle vise à adapter l'Europe aux nouvelles réalités du numérique. Elle poursuit principalement trois objectifs[4], à savoir :

- Le renforcement des droits des personnes ;
- La responsabilisation des acteurs traitant des données personnelles ;
- Une régulation plus crédible grâce notamment à une coopération renforcée entre les autorités de protection des données.

Renforcement des droits des personnes

En ce qui concerne les droits des personnes, le règlement prévoit :

- Plus de transparence dans la mise en œuvre des traitements de données (articles 12 à 15) et un renforcement du consentement des personnes concernées par ces traitements (articles 7 et 8) ;
- De nouveaux droits, comme le droit à la portabilité des données[5] (articles 16 à 22)[6].

[1] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

[2] La Loi Informatique et Libertés de 1978 sera cependant modifiée en 2018 pour s'adapter au GGPD (voir le dossier de procédure législative : http://www.assemblee-nationale.fr/15/dossiers/donnees_personnelles_protection.asp

[3] https://www.cnil.fr/fr/adoption-du-reglement-europeen-par-le-parlement-europeen-un-grand-pas-pour-la-protection-des-donnees.

[4] https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels.

[5] Le droit à la portabilité des données permet à une personne de récupérer les données la concernant sous une forme réutilisable pour pouvoir, le cas échéant, les transférer à un tiers (https://www.cnil.fr/fr/le-droit-la-portabilite-en-questions). Ces droits s'ajoutent à ceux déjà en vigueur (lisibilité, droit d'accès, droit de rectification, droit à l'oubli).

[6] https://www.cnil.fr/fr/plus-de-droits-pour-vos-donnees.

- De nouvelles voies de recours avec les actions collectives[7] et le droit à réparation des dommages matériels ou moraux du fait d'une violation du RGPD (articles 77 à 82).

Responsabilisation des acteurs

Le RGPD repose sur une logique de conformité qui remplace la notion de « formalités préalables » de la directive de 1995. Les responsables des traitements ne sont donc plus soumis à des mesures de déclaration ou d'autorisation. En revanche, ils doivent pouvoir démontrer à tout moment la conformité de leurs traitements au RGPD, ce qui implique de respecter certaines obligations :

- Assurer la protection des données dès la conception du produit ou du service et par défaut (articles 24 et 25) ;
- Tenir un registre des traitements mis en œuvre (article 30) ;
- Sécuriser les traitements et notifier toute violation de données personnelles (articles 32 à 34) ;
- Désigner un délégué à la protection des données (DPD)[8] dans les cas où le responsable du traitement appartient au secteur public (hors cadre juridictionnel) ou que ses activités concernent le suivi des personnes à grande échelle ou qu'elles concernent des données « sensibles »[9] (articles 37 à 39) ;

Notons que le Règlement prévoit que le droit national pourra préciser des conditions spécifiques pour certains traitements, notamment le maintien d'un régime d'autorisation comme pour les données de santé par exemple (article 9 et articles 85 à 91). En outre, il introduit deux nouvelles obligations lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes : la réalisation d'une étude d'impact sur la vie privée et, le cas échéant, une consultation préalable de l'autorité de contrôle (articles 35 et 36). Enfin, les sous-traitants sont désormais tenus de respecter les mêmes obligations que les responsables des traitements en matière de sécurité (articles 28).

Renforcement du contrôle et des sanctions

Les autorités de contrôle comme la CNIL en France, disposeront davantage de pouvoirs pour contrôler la conformité des traitements (articles 51 à 59). Elles pourront notamment :

- Prononcer un avertissement ou mettre en demeure les responsables ;
- Limiter temporairement ou définitivement un traitement ou encore suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ou la rectification, la limitation ou l'efface des données ;
- Infliger des amendes administratives pouvant s'élever jusqu'à 10 ou 20 millions d'euros, ou dans le cas des entreprises, jusqu'à 2% ou 4% de leur chiffre d'affaires annuel mondial (article 83).

Par ailleurs, le RGPD renforce la coopération entre les autorités de contrôle des États membres (articles 60 à 76). D'une part, il permet aux autorités de contrôle de se prêter mutuellement assistance et de réaliser des

[7] Les actions collectives offrent la possibilité à des associations agissant pour la protection des données d'introduire des recours devant des juridictions comme en matière de protection des consommateurs.

[8] https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees.

[9] Sont considérées comme sensibles les données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques, les données concernant la santé ou celles concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique (article 9).

opérations conjointes. D'autre part, il crée un Comité européen de la protection des données (CEPD), qui réunit l'ensemble des autorités de contrôle et qui a vocation à remplacer l'actuel G29.

Transferts de données et traitements hors UE

Le règlement a une portée extraterritoriale en ce qu'il encadre les transferts et les traitements de données hors de l'UE (articles 44 à 50). Il autorise les transferts de données hors de l'UE et leurs traitements à la condition que les responsables assurent un niveau conforme de protection des personnes. En outre, les données transférées restent soumises au droit de l'UE.

Enjeux relatifs à l'application du RGPD

Avec l'entrée en application du RGPD, l'UE souhaite s'adapter aux évolutions de la société numérique tout en assurant un haut niveau de protection des personnes. Néanmoins, le RGPD est-il compatible avec la rapide transformation numérique ?

La sécurité des données est au cœur de la conformité au RGPD. A ce titre, quels peuvent être les impacts du nouveau Règlement en matière de cybersécurité ?

Enfin, la portée extraterritoriale du texte s'inscrit nécessairement dans les enjeux de la gouvernance du cyberespace. Ainsi, quelles peuvent être les implications du RGPD dans la géopolitique des données ?

Compatibilité du RGPD avec la transformation numérique

Si les contraintes qu'impose le RGPD soulèvent des inquiétudes pour le développement des innovations technologiques en Europe, des experts jugent que le texte constitue, au contraire, une opportunité pour la transformation numérique européenne.

Des inquiétudes pour le développement des innovations technologiques…

Les nouvelles règles contraignantes du RGPD pourraient, par exemple, constituer un obstacle pour le développement de l'intelligence artificielle (IA) en Europe[10]. D'une part, le principe du consentement et les droits des personnes pourraient venir limiter l'alimentation continue en données nécessaire à l'IA. D'autre part, les analyses de l'IA se basent sur des corrélations dont les impacts sur la vie privée ou sur la conformité d'un traitement de données personnelles peuvent être difficiles à prévoir.

Ainsi, le RGPD pourrait freiner les entreprises européennes en matière d'innovation alors que l'UE accuse déjà un retard dans le développement de l'IA vis-à-vis des GAFA américains ou des BATX chinois[11]. Par ailleurs, ces derniers pourraient ne pas proposer leurs nouveaux services basés sur l'IA en Europe. Notons à

[10] https://www.challenges.fr/high-tech/rgpd-protection-des-donnees-et-big-data-l-europe-tourne-le-dos-a-l-innovation_560889

[11] http://www.zdnet.fr/blogs/green-si/rgpd-epee-de-damocles-sur-l-innovation-europeenne-39861998.htm

ce propos que Facebook ne propose pas certaines fonctionnalités utilisant la reconnaissance faciale et l'IA en Europe en partie en raison du cadre juridique européen sur la protection des données[12].

L'application du RGPD à la technologie blockchain pose également des difficultés. Si pour les blockchains privées, aucun problème de conformité ne devrait se poser du fait qu'elles sont gérées par un tiers[13], certaines caractéristiques des blockchains publiques sont incompatibles avec le RGPD[14]. En effet, la blockchain publique est par définition décentralisée, il n'y a donc aucun responsable de traitement. En outre, il n'est pas possible d'effacer les données, ce qui entre en contradiction avec le principe de conservation limitée des données ou encore avec le droit à l'oubli du RGPD.

Ou une opportunité pour la transformation numérique européenne

Certains experts considèrent que le RGPD constitue, au contraire, une opportunité pour la transition numérique en Europe et que les inquiétudes sur l'application du texte aux innovations technologiques ne sont pas fondées[15]. Bien que le RGPD impose des contraintes importantes pour les responsables des traitements, il permettrait à ces derniers de mieux analyser les risques qui pèsent sur les données et d'augmenter le niveau de confiance, ce qui pourrait constituer un avantage concurrentiel. En outre, les mesures qu'impose le RGPD devraient contribuer à mieux identifier les données pertinentes pour le fonctionnement du Big Data ou de l'IA[16].

RGPD et cybersécurité

En introduisant des règles contraignantes en matière de sécurité des systèmes d'information, le RGPD devrait contribuer au renforcement de la cybersécurité en Europe. En effet, les organismes devront être en mesure d'assurer la sécurité de leurs traitements de données personnelles au risque d'être sévèrement sanctionné par les autorités de contrôle.

Obligations de sécurité à la charge des organismes

S'il n'existe généralement pas de règles contraignantes pour les organismes en matière de cybersécurité (sauf pour certains acteurs comme par exemple les autorités administratives ou les opérateurs d'importance vitale en France[17]), le RGPD oblige désormais tous les organismes qui traitent des données personnelles à prendre des mesures techniques et organisationnelles contre les risques de violation de données personnelles, qu'ils

[12] http://www.zdnet.fr/actualites/facebook-pas-en-europe-nouvelle-arme-du-reseau-social-39861874.htm

[13] https://linc.cnil.fr/fr/blockchain-et-rgpd-une-union-impossible-0

[14] http://www.journaldunet.com/economie/finance/1207079-la-blockchain-est-elle-compatible-avec-rgpd/

[15] http://www.zdnet.fr/actualites/la-conformite-au-rgpd-est-elle-compatible-avec-la-transformation-numerique-39860720.htm

[16] https://www.infosecurity-magazine.com/opinions/gdpr-innovation-deterrent-incentive/

[17] En France, l'ordonnance 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives met en place le Référentiel général de sécurité (RGS) qui s'impose aux autorités administratives et la loi de programmation militaire de 2013 définie des mesures de cybersécurité pour les opérateurs d'importance vitale (OIV).

soient accidentels ou volontaires[18]. En plus de consacrer le concept de « privacy by design » (article 25), il mentionne un certain nombre de mesures de sécurité à prendre (article 32) :

- La pseudonymisation et le chiffrement des données ;
- Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- Des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;
- Des mesures permettant de garantir que le personnel relevant de l'autorité du responsable du traitement ou de celle du sous-traitant, qui a accès à des données personnelles, ne les traite pas de manière non autorisée.

Rappelons également que les organismes ont l'obligation de notifier aux autorités de contrôle toute violation de données personnelles (article 33).

Les mesures à prendre pour assurer le niveau de sécurité attendu par le RGPD peuvent impliquer des changements importants pour un organisme (actions correctives, mise en place d'une stratégie de gestion des risques ou mise en place de monitoring continu pour améliorer les procédures liées à la maîtrise des risques), ce qui peut susciter des inquiétudes ou des difficultés (techniques, organisationnelles et humaines, juridiques et budgétaires)[19].

Le RGPD introduit ainsi une nouvelle culture de la protection des données et de la sécurité des traitements. Avec l'application de la notion de « *privacy by design* » et la nécessité de sécuriser les traitements, c'est aux organismes qu'il incombe en premier lieu la charge de protéger les données des personnes[20]. Aussi, dans le cadre du débat sur le chiffrement, le RGPD semble avoir pris position en faveur de sa généralisation. Enfin, la nécessité de prendre des mesures techniques pour assurer la sécurité des traitements pourrait profiter aux acteurs qui proposent des solutions de cybersécurité, notamment dans un contexte d'augmentation des cyberattaques[21].

Contrôle des autorités sur la sécurité des traitements

Les nouvelles obligations qu'impose le RGPD en matière de cybersécurité implique qu'une part importante du contrôle des autorités devrait porter sur les systèmes d'information. En effet, les autorités auront la tâche de contrôler la conformité des mesures techniques et organisationnelles prises par les organismes pour assurer la sécurité de leurs traitements. En outre, elles seront chargées de recueillir les notifications de violation de données personnelles et de vérifier si les mesures de sécurité adéquates ont été prises. Soulignons que pour les violations des obligations de sécurité, les autorités de contrôle peuvent désormais prononcer des amendes

[18] https://fr.business.f-secure.com/ce-que-le-rgpd-dit-a-propos-des-ransomware/

[19] https://www.challenges.fr/entreprise/rgpd-l-union-europeenne-renforce-sa-position-sur-la-securite-des-donnees-personnelles_474627

[20] https://www.linformaticien.com/dossiers/rgpd-et-securite.aspx#suite

[21] https://www.silicon.fr/securite-informatique-marche-cyberattaques-rgpd-193049.html?inf_by=5a844f75671db840308b4fbc

administratives pouvant s'élever jusqu'à 10 000 000 d'euros ou jusqu'à 2% du chiffre d'affaires annuel mondial total d'une entreprise.

Ainsi, le contrôle et les sanctions prévus par le RGPD devraient fortement inciter les organismes à adopter des mesures de cybersécurité pour protèges les données personnelles et à coopérer avec les autorités de contrôle. Elles devraient également inciter ces dernières à renforcer leurs compétences et leurs qualifications en matière de sécurité des systèmes d'information.

Face à ces nouvelles missions, il pourrait être nécessaire de donner plus de moyens aux autorités de contrôle. Ainsi, pour la présidente de la CNIL, Isabelle Falque-Pierrotin, il est indispensable de renforcer les moyens de l'institution, notamment pour permettre d'accompagner et suivre les organismes dans leur démarche de conformité mais aussi pour satisfaire au renforcement de la coopération entre les autorités européennes de protection prévue par le RGPD[22].

Transferts de données hors UE et géopolitique des données

Les modifications apportées par le RGPD sur le cadre juridique des transferts de données hors de l'UE devraient faciliter la circulation des données personnelles. Néanmoins, cette liberté de circulation implique pour les pays tiers et leurs organismes d'adopter des mesures cohérentes avec les règles du RGPD.

Liberté de circulation des données personnelles hors de l'UE

Jusqu'à présent, les transferts de données personnelles hors de l'UE ne pouvait avoir lieu, en principe, que si le pays tiers concerné était en mesure d'assurer un niveau de protection adéquat[23]. Avec le RGPD, ces transferts sont par principe autorisés vers les pays tiers ou les organisations internationales lorsque les responsables de traitement et les sous-traitants encadrent ces transferts avec des outils assurant un niveau de protection suffisant et appropriés des personnes.

A ce titre, le RGPD prévoit un certain nombre d'outils juridiques permettant aux responsables de traitement et aux sous-traitant de transférer des données hors UE sans qu'il soit nécessaire d'obtenir une autorisation préalable de l'autorité de contrôle (article 46). Ces outils comprennent notamment :

- Des règles d'entreprises contraignantes ;
- Des clauses contractuelles types approuvées par la Commission européenne ;
- Des clauses contractuelles adoptées par une autorité de contrôle et approuvées par la Commission européenne.

Impacts du RGPD pour les pays tiers et leurs organismes

Si le RGPD facilite la circulation des données personnelles hors de l'UE, il étend également ses obligations aux organismes situés dans les pays tiers. En effet, les responsables de traitement ou sous-traitants situés

[22] http://www.lefigaro.fr/secteur/high-tech/2018/01/22/32001-20180122ARTFIG00326-isabelle-falque-pierrotin-la-cnil-manque-de-moyens-face-a-ses-nouvelles-missions.php

[23] Article 25 de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

dans un pays tiers qui traitent des données personnelles de ressortissants de l'UE devront se conformer aux obligations du RGPD. A ce titre, le Règlement devrait donc avoir un impact sur les stratégies internationales des entreprises. Si certaines d'entre elles pourraient y voir un atout concurrentiel, d'autres pourraient vouloir échapper aux contraintes qu'imposent le RGPD. Dans le cas où la majorité des entreprises établies hors UE s'accorderaient avec le droit de l'UE, le RGPD pourrait devenir une norme de référence internationale pour la gouvernance des données personnelles mais aussi en matière de cybersécurité[24]. En revanche, dans le cas contraire, le RGPD conduirait davantage à une segmentation du cyberespace et potentiellement à une transformation numérique à plusieurs vitesses. Par exemple, les États-Unis offriraient un environnement favorable pour un cyberespace pour les entreprises et l'Union européenne, un environnement favorable pour un cyberespace pour les personnes[25].

Par ailleurs, au-delà des entreprises, le RGPD pourrait impacter les relations entre l'UE et les États tiers. Ces derniers, s'ils souhaitent conserver ou développer leurs échanges de données avec les pays de l'UE, devront satisfaire aux enjeux du RGPD (mise en place d'une autorité de contrôle et adoption d'une loi sur la protection des données par exemple). En effet, la non-conformité d'entreprises d'un pays tiers pourrait avoir des impacts sur son économie[26]. Les sanctions importantes que peut prononcer l'UE à l'encontre d'une entreprise ressortissante d'un pays tiers pourraient d'ailleurs créer des tensions.

En France, consciente que la mise en conformité est un processus lourd et exigeant qui suscite des inquiétudes, la CNIL se veut rassurante en soulignant qu'elle fera preuve de souplesse en matière de contrôle et qu'elle accompagnera les entreprises dans leur démarche même après le 25 mai, date d'entrée en application du RGPD[27]. Une démarche similaire pourrait être adoptée concernant l'application extraterritoriale du texte afin d'éviter des tensions, notamment avec les pays tiers partenaires de l'UE.

[24] http://www.information-age.com/gdpr-catalyst-global-digital-transformation-123462192/

[25] http://www.zdnet.fr/blogs/green-si/rgpd-epee-de-damocles-sur-l-innovation-europeenne-39861998.htm

[26] https://www.webmanagercenter.com/2018/02/17/416370/liste-noire-rgpd-le-prochain-casse-tete-pour-leconomie-tunisienne/

[27] https://www.latribune.fr/technos-medias/internet/rgpd-la-position-de-la-cnil-sera-souple-au-debut-769003.html

RESEAUX SOCIAUX ET POUVOIRS PUBLICS AU DEFI DU CYBERJIHADISME

Au cours des années 2000, Internet est devenu l'outil de propagande jihadiste par excellence : les sites web et forums dédiés, en arabe d'abord puis en anglais et désormais traduits dans une multitude de langues, ont rapidement remplacé les flyers, tracts et autres publications. L'insurrection syrienne de 2011 et l'arrivée de jeunes européens familiers des réseaux sociaux grand public et qui en ont démocratisé l'usage sur le terrain ont marqué un nouveau tournant : les années 2011-2015 ont ainsi vu déferler les contenus jihadistes sur les réseaux sociaux, facilitant la propagande, le recrutement, et incitant au terrorisme.

Réseaux sociaux et pouvoirs publics sont donc tous deux concernés par ce phénomène de « cyberjihadisme ». Les réseaux sociaux d'abord, parce que c'est principalement grâce à (et sur) leurs plateformes que circulent les contenus terroristes. Les pouvoirs publics ensuite, car la lutte contre la propagande jihadiste en ligne est l'un des piliers des politiques de lutte contre le terrorisme.

Le contrôle et la régulation de ces contenus à caractère terroriste constituent donc une priorité pour les pouvoirs publics à laquelle se sont finalement ralliés les réseaux sociaux, les placent face à plusieurs défis. Des défis juridiques d'abord, puisque la nature exacte du contenu concerné mais aussi les rôles et responsabilités et les modalités et outils d'action de chacun ne sont pas clairement définis et délimités par la loi. Des dilemmes opérationnels et stratégiques ensuite, car le contrôle des contenus fait partie à part entière du dispositif de lutte contre le terrorisme. Des enjeux technologiques, humains et organisationnels enfin, car la lutte contre le cyberjihadisme implique de se doter de moyens technologiques adaptés et de mécanismes de coordination des acteurs et des moyens.

Le cyberjihadisme : un phénomène encore difficile à apprécier juridiquement qui pose de réels défis technologiques et humains

Identification et qualification : un flou juridique déstabilisant

Au regard du droit français, les contenus à caractère terroriste sont soumis au régime juridique des contenus dits « illicites » car contraires à l'ordre public et présentant un danger pour les populations exposées. Ils sont régis par la loi du 21 juin 2004 pour la confiance dans l'économie numérique qui sanctionne notamment « la provocation à la commission d'actes de terrorisme et leur apologie » et prévoit leur retrait. Or, la définition même d'un contenu à caractère illicite, ou dans ce cas à caractère terroriste, est loin d'être non équivoque. Par exemple, il est parfois difficile de distinguer ce qui relève de la simple provocation, de la propagande ou de l'incitation au terrorisme à proprement parler. Et quid des contenus repris par des analystes, chercheurs et experts de la lutte contre le cyberjihadisme pour alerter sur les publications et propos dangereux émis par certains comptes? Si la question de la qualification est aussi importante, c'est que la jurisprudence n'exige de mesures de retrait que pour les seuls contenus à caractère « manifestement » illicite. Les contenus sur lesquels il est plus difficile de statuer sont donc situés dans une « zone grise » et nécessitent une analyse plus poussée et une remise en contexte. Cette disposition vise à limiter les sanctions automatiques et abusives mais n'évite pas certaines erreurs: un nombre toujours trop important de comptes émetteurs de contenus

dangereux sont encore actifs alors que certains experts ont pu être sanctionnés pour avoir republié à des fins d'alerte ou d'analyse des contenus émis par d'autres. Ce constat soulève la question des outils de détection et de leur réelle efficacité.

Détection et signalement : les limites des outils technologiques et l'indispensable intervention humaine

La détection de contenus jihadistes repose sur des moyens humains aussi bien que techniques. Elle peut d'abord être effectuée par tout utilisateur des réseaux sociaux exposé à ce type de contenu, qui peut ensuite le signaler soit directement sur la plateforme du réseau considéré selon ses règles d'utilisation (par exemple le bouton « report » sur Youtube), soit anonymement sur des plateformes publiques comme « pointdecontact.net » de l'Association Française des Prestataires d'Internet (AFPI) ou PHAROS du ministère de l'Intérieur. Ce système trouve toutefois ses limites dans le nombre finalement réduit d'utilisateurs exposés directement à ces contenus, sur lesquels les pouvoirs publics peuvent donc compter pour signaler des publications suspectes.

Pour faire face à une volumétrie en constante augmentation des contenus à caractère jihadiste, les réseaux sociaux ont donc développé des dispositifs de détection automatisée qui s'appuient sur les technologies de l'intelligence artificielle. C'est le cas notamment de Twitter, dont les règles d'utilisation interdisaient déjà de facto les publications à caractère terroriste sous la qualification « appel à la violence », mais qui s'est doté, après les attaques terroristes de 2015, d'outils propriétaires de détection de contenus basés sur ses instruments de détection des spams. De même, Google et sa plateforme de partage de vidéos Youtube utilisent le machine learning et le photo matching de façon de plus en plus performante pour détecter les contenus cyberjihadistes. Ces instruments permettent même de dégager des faisceaux d'indice indiquant qu'un compte ou un profil ont pour unique finalité la diffusion de propagande jihadiste et de les bloquer avant même qu'ils n'aient pu publier. Les résultats sont sans appel : au 31 décembre 2017, plus d'1,5 millions de comptes Twitter émetteurs de contenus jihadistes avaient été supprimés. 73% l'avaient été grâce aux outils de détection automatique dont trois quart avant même l'envoi du premier tweet. De même, dans les 6 premiers mois de 2017, 50% des contenus relevant de l'incitation au terrorisme avaient été retirés de la plateforme Youtube grâce à l'intelligence artificielle (IA). Toutefois, si l'IA devient de plus en plus rapide et précise dans la détection de contenus illicites, le traitement automatisé des contenus est toujours susceptible de générer des « faux positifs » ou de faire remonter des contenus qui ne seraient pas « manifestement illicites ». L'intervention humaine reste donc nécessaire pour re-contextualiser les publications, affiner les résultats des outils technologiques, et traiter de la façon la plus précise et juste possible les contenus difficiles à qualifier. Ceci explique la présence d'équipes dédiées au sein des réseaux sociaux et plateformes concernés, dont le rôle est d'analyser puis de statuer sur la nature du contenu signalé ou détecté avant de prendre les mesures de modération nécessaires.

Et les enjeux sont de taille : une fois qualifiés comme tels, les contenus à caractère jihadiste ou les comptes émetteurs peuvent être supprimés, c'est à dire censurés. Ces mesures radicales ne sont pas sans avoir de conséquences tant au plan opérationnel que stratégique, dans le succès de la lutte contre le cyberjihadisme.

Contrôle et régulation : les enjeux de la modération

Dans le cadre d'opérations dont le but est de contrer la propagation de ces discours de propagande, supprimer un compte émetteur de contenu à caractère jihadiste, ou retirer/bloquer un contenu de même nature permet de déstabiliser son auteur, de le ralentir, de l'obliger à se réorganiser et à redéployer des ressources pour être en mesure de continuer à diffuser, et donc de l'affaiblir en diminuant la portée de ses publications et par extension de ses activités de propagande. Mais dans le cadre d'opérations de renseignement ou d'enquêtes judiciaires, les comptes et contenus à caractère jihadiste constituent autant de sources ouvertes qu'il est aisé et utile d'exploiter. Les supprimer force leurs auteurs à se replier vers des plateformes moins accessibles, privant ainsi les agents du renseignement de canaux d'informations et rendant les enquêtes d'autant plus délicates. Depuis 2015, l'accélération des contrôles effectués par les pouvoirs publics a forcé les auteurs de propagande jihadiste à se replier vers d'autres plateformes plus confidentielles comme Telegram et autres messageries chiffrées. Maîtrisant à la perfection les réseaux sociaux, ils ont rapidement appris à exploiter et tirer profit des outils garantissant un certain degré de clandestinité – et donc de sécurité, ou du moins de confort : chaînes de diffusion plus ou moins visibles et accessibles, liens révocables ou à durée de vie limitée… Les plateformes du deep et du darkweb comptent également parmi les options de repli privilégiées pour les auteurs de contenus les plus radicaux et les plus virulents, qui deviennent ainsi plus difficile à détecter.

Ensuite, la suppression systématique d'un contenu ou le blocage d'un compte ou d'un profil par les plateformes et hébergeurs reste assimilable à une forme de censure qui va à l'encontre de la raison même d'être de ces réseaux sociaux : mettre à disposition des utilisateurs des plateformes et forums leur permettant d'exprimer des idées et opinions diverses. Supprimer un compte ou un contenu peut donc être considéré comme une atteinte à la liberté d'expression et une forme de stigmatisation. D'autant que laisser aux plateformes et aux réseaux sociaux le soin de statuer sur la licéité d'un contenu avant de le retirer revient à leur attribuer des rôles et responsabilités qui relèvent normalement des autorités régaliennes, ce qui pose la question de leur légitimité en matière de contrôle de contenu.

La situation est toutefois différente quand il s'agit de demandes émanant du ministère de l'Intérieur et exigeant des hébergeurs qu'ils retirent le contenu illicite ou enjoignant les fournisseurs de le bloquer. Mais dans ce cas également la régulation des contenus intervient hors de tout cadre juridique, puisque depuis 2014, les agents du ministère de l'Intérieur sont habilités à agir rapidement, c'est-à-dire sans ouverture d'enquête judiciaire, pour demander, sous le contrôle de la CNIL, le blocage d'office des contenus signalés et qualifiés d'apologétiques. La lutte contre le cyberjihadisme est à ce titre au centre du dilemme sécurité/liberté et la modération d'un contenu à caractère terroriste peut s'avérer délicate. Des solutions alternatives sont donc déployées pour compléter ce dispositif et contrer la propagation de contenu de propagande et d'incitation au jihadisme.

Les dispositifs alternatifs de modération

Les plateformes et réseaux sociaux ont mis en place des mesures moins définitives et radicales que le retrait de contenus ou la suppression de comptes. Pour certains contenus qui ne sont illicites que dans certains pays, Google utilise le géo-blocage, qui permet de masquer le contenu localement. D'autres dispositifs visent à

limiter la viralité de certains contenus, comme par exemple le retrait des recommandations de contenus similaires ou associés sur les pages web, et d'autres encore ont pour objectif de sensibiliser et alerter les individus exposés sur le caractère controversé ou dangereux d'un contenu. Pour aller plus loin et participer activement à la lutte contre le jihadisme, les plateformes et réseaux sociaux se sont engagés à contribuer à la construction d'un contre-discours, en écho aux politiques et campagnes menées par les autorités. Ainsi Google, via l'outil Redirect de sa branche Jigsaw, associe aux mots-clés redirigeant habituellement vers des contenus illicites, des contenus pédagogiques relayant ce contre-discours.

Le défi de la coopération : entre collaboration et coordination

Une collaboration nécessaire mais pas automatique

L'efficacité du dispositif de lutte contre le cyberjihadisme dépend également des efforts coopération entre réseaux sociaux et pouvoir publics. Les autorités chargées du respect de l'ordre public et de la lutte contre le terrorisme doivent en effet pouvoir compter sur les plateformes et réseaux sociaux, d'abord parce que leurs outils de détection sont plus sophistiqués et plus performants, ensuite parce que seuls les hébergeurs et fournisseurs ont techniquement la capacité de bloquer, supprimer ou retirer un contenu ou un profil. Des plateformes comme Twitter, Google ou Facebook, ont enregistré une augmentation croissante du nombre de demandes de suppression de compte venant des États. Quant aux entreprises du numérique qui disposent certes des moyens techniques nécessaires, mais n'ont pas toute la légitimité nécessaire pour exercer cette forme de censure qu'elles appliquent de facto, elles doivent pouvoir s'appuyer sur une collaboration affichée avec les autorités dans le cadre de la lutte contre le terrorisme pour légitimer leurs actions de modération. Plus les mesures de modération sont effectuées à la demande des autorités, et moins elles sont contestables.

Mais tous ne sont pas aussi coopératifs. Si certains comme Twitter et Google font figure de bons élèves avec des délais de retrait pouvant être aussi courts que 3 minutes, d'autres comme Telegram, qui ont un historique et des relations plus délicates avec les autorités sont beaucoup moins réactives et collaborent plus difficilement, voire pas du tout. D'autre part, certains points d'achoppement continuent à freiner la coopération entre réseaux sociaux et pouvoirs publics en matière de lutte contre le cyberjihadisme. Par exemple, la question du chiffrement pose de véritables difficultés car les réseaux sociaux refusent encore l'accès aux messageries chiffrées et continuent d'innover pour sécuriser les conversations de leurs utilisateurs, notamment via la mise en place du chiffrement de bout en bout sur certaines applications, comme Messenger (Facebook) en 2016.

Dispositifs de coordination et moyens d'action communs

C'est pour répondre à ces défis que réseaux sociaux et pouvoirs publics ont mis en place, dès 2015, des mécanismes de coopération leur permettant d'atteindre ensemble des objectifs communs. En France, le protocole Cazeneuve de 2015 a ainsi rassemblé les services de l'État et les géants du numérique, habituellement plutôt défiants, dans un groupe de contact permanent qui se réunit tous les deux mois pour aborder des problématiques communes et constitue une instance de dialogue de la lutte contre le cyberjihadisme. De même, l'Allemagne a renforcé sa législation sur la modération des contenus en 2015, et

les États-Unis ont intensifié leur coopération avec Facebook début 2016 suite à la tuerie de Bernardino. La même année, Facebook, Twitter, YouTube, Microsoft se sont engagés auprès de la Commission européenne à examiner en moins de 24 heures les signalements demandant la suppression de contenus. Dans le même ordre d'idées, la création du Global Internet Forum to Counter Terrorism, à l'initiative du EU Internet Forum et de Facebook, Microsoft, Twitter et YouTube, étend ces efforts de coopération et coordination à l'échelle internationale.

Pour être effective, la lutte contre la propagation de contenus à caractère terroriste nécessite donc l'intervention et l'implication combinées et coordonnées des réseaux sociaux et des pouvoirs publics dont les prérogatives et capacités sont complémentaires même si leurs intérêts ne se recoupent pas entièrement. Tout l'enjeu est donc d'affiner et perfectionner les mécanismes leur permettant d'allier leurs forces et atouts respectifs, pour faire face aux défis de la lutte contre le cyberjihadisme : respect des libertés individuelles, limitations techniques et technologiques, régime juridique en cours d'élaboration…

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis.eu