Def'INSEEC
Pole Aerospace & Cybersecurity

La régulation du Cyberespace dans l'Union Européenne

Cybersécurité et Cybercrimes

Temps de lecture : 15min

DEF'INSEEC DEFINSEEC@GMAIL.COM 06 66 73 71 65

INTRODUCTION

La protection contre les cyber-attaques représente un des enjeux majeurs des années à venir dont les Etats prennent doucement conscience. L'Union Européenne (UE), dans son objectif de promotion de la cohésion économique, sociale et territoriale et de la solidarité entre Etats membres, a établi des objectifs de coordination et de coopération en matière de cybersécurité. Les premières mentions de cyber-préoccupations par l'UE se font dès 2001 à travers la Convention de Budapest sur la Cybercriminalité. Elaborée et adoptée par le Conseil de l'Europe, elle tente d'aborder les crimes informatiques et sur Internet notamment la pornographie infantile, l'atteinte aux droits d'auteur et les discours de haine. Son but est d'améliorer les techniques d'enquêtes et d'augmenter la coopération par une harmonisation entre Nations. Aujourd'hui, 63 pays dont la France ont signé cette Convention qui est la première contraignante en la matière et à vocation internationale.

C'est donc d'abord par la reconnaissance de cyber-crimes, d'infractions liées de manière générale à l'utilisation des nouvelles technologies, que l'UE va inscrire l'importance de l'établissement d'une cybersécurité. Celle-ci va occuper une place de plus en plus grande dans la Politique Etrangère et de Solidarité Commune (PESC) passant de simple mention à volet à part entière. La cybersécurité est "l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyber espace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessible" selon l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI).

En 2016, 80% des entreprises européennes ont connu un incident lié à la cybersécurité. On évalue au niveau mondial l'impact économique des cyber-attaques à 400 millions d'euros par an selon la Commission Européenne, c'est donc une priorité que l'on ne peut ignorer. Dès lors, comment l'UE est-elle passée d'un soutien à la compétence, à la lutte contre la fraude ? En effet, dans ses premiers pas vers l'établissement d'une cyberdéfense, l'UE a d'abord soutenu les instances nationales dans l'approfondissement de leurs plates-formes de signalement chargées de la lutte contre la cybercriminalité. Elle a ensuite établi une protection des individus par la protection de leurs données et des produits et enfin, a mis en place des organismes et mécanismes européens chargés de la sécurité des réseaux, de l'information et des produits.

Par conséquent, l'Union Européenne (UE) est passée d'un soutien à la compétence à la lutte contre la fraude en commençant par l'encadrement des réseaux et des systèmes d'information pour enfin arriver à la protection cette fois-ci des individus et des produits d'entreprises.

De l'encadrement des réseaux et des systèmes d'informations...

Du protocole de Stockholm à la directive sur la sécurité des réseaux et des systèmes d'information

D'une part, l'UE soutient la compétence des Etats membres en ce qui concerne les techniques d'enquête pour la cybercriminalité. Mais, dès 2010, l'UE prend conscience de la nécessité d'approfondir ces techniques ainsi que la coopération entre Nations. C'est à travers **le programme de Stockholm,** une Europe ouverte et sûre qui sert et protège les citoyens, que ce changement se fait sentir. Etablie par le Conseil Européen et adressé à la Commission Européenne et au Conseil de l'Europe, il aborde la problématique de la cybercriminalité qui nous renvoie d'abord à la Convention de Budapest sur la Cybercriminalité que nous aborderons plus en profondeur plus loin (*page 7)*. Puis, le Conseil Européen invite la Commission à "faire des propositions pour clarifier, si nécessaire, le cadre juridique en matière d'enquêtes dans le cyberespace au sein de l'Union". Il invite également Europol "à jouer un rôle à cet égard en tant que centre de ressources européen par la création d'une plate-forme européenne de signalement des infractions qui devrait aussi aider les plates-formes nationales de signalement des États membres à échanger les meilleures pratiques". Les prémices d'une réglementation et d'une entité encadrant le cyber espace sont alors établies.

C'est après un travail de longue haleine pendant près de six années, que la directive sur la sécurité des réseaux et des systèmes d'information (SRI) entre en vigueur en août 2016 avec un délai de transposition allant jusqu'au 9 mai 2018.C'est la première législation européenne sur la cybersécurité. Le but de cette directive est de garantir un niveau de sécurité des réseaux et systèmes d'information uniformément élevé dans l'ensemble de l'UE par une amélioration des capacités nationales en matière de cybersécurité, un renforcement de la coopération à l'échelle de l'UE et l'instauration d'obligations de gestion des risques et de notification des incidents pour les opérateurs de services essentiels et les fournisseurs de services numériques. Cette directive oblige également les Etats membres à désigner une ou plusieurs autorité(s) nationale(s) chargée(s) de contrôler l'application de cette directive et à se doter d'une stratégie pour la lutte contre les cybermenaces notamment les incidents de sécurité des réseaux et des systèmes d'information qui minent la confiance des utilisateurs.

Le support d'une entité chargée de la sécurité des réseaux et de l'information : l'approfondissement de l'ENISA.

L'ENISA est chargée de la sécurité des réseaux et de l'information et soutient donc la directive précédemment décrite. Créée en 2004 et n'ayant qu'un rôle analytique à sa création, elle est placée sous l'autorité d'un conseil d'administration composé de représentants des 28 Etats membres de l'UE et de deux représentants de la Commission européenne et siège à Heraklion en Grèce. Elle a, après la directive de 2016, pour objectif de garantir le plus haut degré de sécurité des réseaux et de l'information et exerce une fonction de conseil et de coordination des mesures prises par la Commission et les pays de l'UE. L'ENISA voit le jour car les réseaux informatiques ont subi des violations de leurs sécurités ayant provoqué des dommages financiers considérables et ébranlés la confiance des utilisateurs. L'objectif de l'UE, par la création de l'ENISA est donc de renforcer sa capacité et celle du secteur privé des entreprises en matière de prévention, de réaction et de gestion des problèmes liés à la sécurité des réseaux et de l'information. Elle doit également faciliter et encourager la coopération entre les secteurs privé et public.

Mais, l'UE va se voir contrainte de renforcer davantage sa législation due aux cyber-attaques d'ampleur toujours croissante ayant lieu sur le sol européen. Nous pouvons prendre l'exemple de la *Ransomware WannaCry*, attaque informatique ayant touché plus de 300 000 ordinateurs le 12 mai 2017. Elle exploite une faille de sécurité dans les systèmes d'exploitation de Microsoft en retard sur leurs mises à jour de sécurité détectée par la NSA. Le virus établissait un chiffrement des données inaccessibles en échange d'une rançon Bitcoins pour le déchiffrement ayant touché des hôpitaux britanniques à l'entreprise Renault, en passant par des ministères russes. L'UE impose alors ses premières sanctions à la suite de cyberattaques : interdiction de pénétrer sur le territoire de l'UE ainsi qu'un gel des avoirs. Dès lors, l'UE va dépasser l'encadrement et entreprendre une protection plus concrète des utilisateurs et des entreprises : c'est le tournant du *Cybersecurity Act* et du *Règlement Général sur la Protection des Données* (RGPD).

...A la protection de tous les utilisateurs : le Cybersecurity Act et le RGPD

La protection des utilisateurs et de leurs données: le RGPD

D'autre part, le RGPD, entré en application le 25 mai 2018, est une révolution dans la législation européenne, voire internationale, car, pour la première fois, ce sont les utilisateurs que l'on vise à protéger et non plus simplement les réseaux et les systèmes d'information. Il est relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel qui, sous format papier ou numérique, rassemblent "toute information se rapportant à une personne physique identifiée ou identifiable", et à la libre circulation de ces données.

Il symbolise la prise de conscience des données comme étant désormais un "carburant de l'économie" c'est-à-dire qu'on se rend compte du caractère essentiel de ces données pour la croissance économique, la création d'emplois ou encore le progrès sociétal. Le RGPD est composé de trois volets:

- Le règlement général sur la protection des données,
- La directive dite "police" adoptée en 2016 et devant être transposée par les Etats membres avant le 8 mai 2018 qui complète le précédent règlement pour plus de cohérences,
- Une proposition de règlement "vie privée et communications électroniques" afin de parachever la modernisation en matière de protection des données.

Basé sur l'article 16 du Traité sur le Fonctionnement de l'UE (TFUE) disposant que "Toute personne a droit à la protection des données à caractère personnel la concernant" et l'article 7 de la Charte des droits fondamentaux de l'UE qui complète le TFUE en la matière en consacrant le droit de toute personne "au respect de sa vie privée et familiale, de son domicile et de ses communications". Le RGPD endosse désormais un réel rôle de protecteur des libertés et induit de nouvelles logiques de responsabilisation des acteurs du traitement des données.

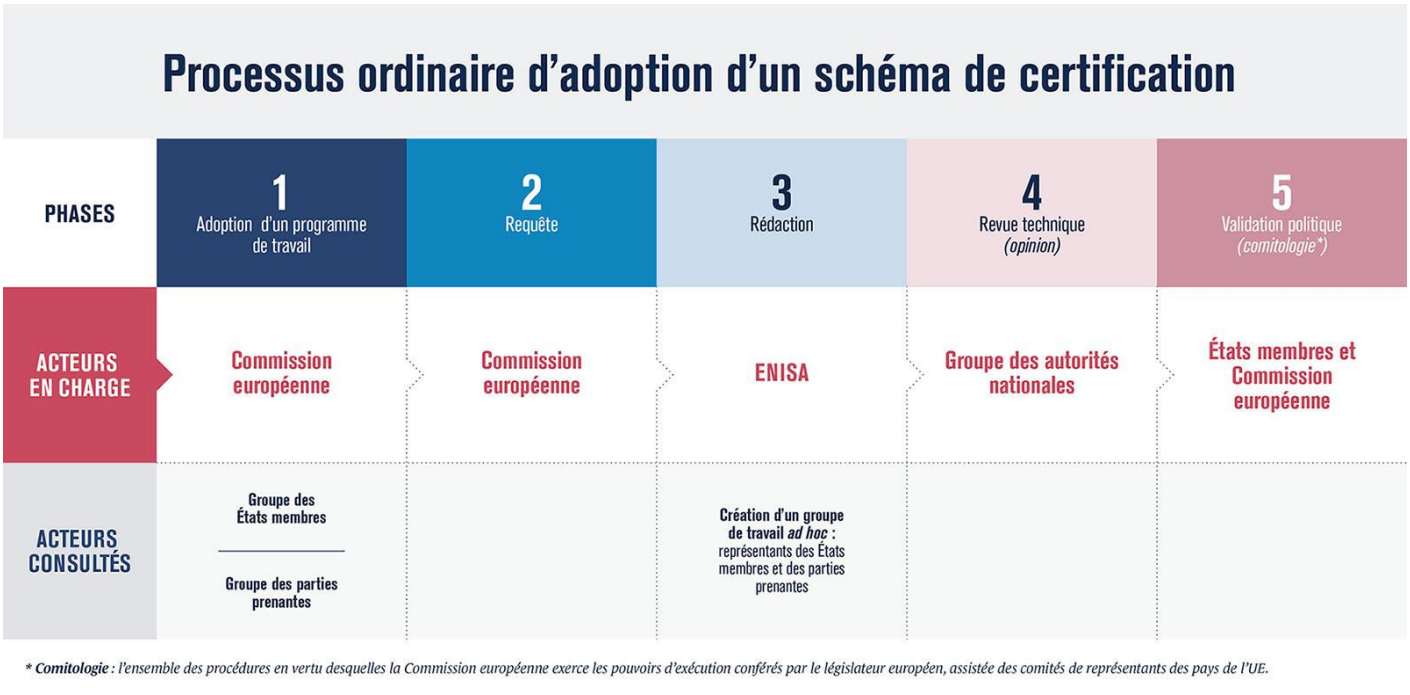
La nécessité d'une cybersécurité performante est, dés lors, intégrée jusque dans les traités. De plus, le RGPD créé le Comité Européen de Protection des Données (CEPD) qui, avec la Cour de Justice de l'UE, veille à une application uniforme dans l'UE du RGPD. Des sanctions sont désormais possibles : rappel à l'ordre, injonction à la mise en conformité, limitation du traitement ou encore une amende Administrative pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondiales de la société visée.

Une harmonisation européenne par la certification : le Cybersecurity Act et la protection des produits

Enfin, le dernier pas de l'UE en matière de cybersécurité passe par le Cybersecurity Act adopté par le Parlement Européen ainsi que par le Conseil de l'UE le 7 juin 2019, règlement à caractère obligatoire et général. Il marque une réelle avancée pour l'autonomie stratégique européenne. Il poursuit un double objectif : l'adoption d'un mandat permanent pour l'ENISA et définit un cadre européen de certification de cybersécurité.

- Le premier volet renomme l'ENISA l'Agence de l'UE pour la cybersécurité et aide les Etats membres à être mieux équipés et préparés pour prévenir et détecter les problèmes de sécurité de l'information et y répondre. L'Agence de l'UE pour la cybersécurité fournit aujourd'hui des conseils pratiques et des solutions aux secteurs publics et privé des Etats membres et aux institutions de l'UE. Elle devient alors un acteur clé en matière d'aide au développement des capacités nationales de cybersécurité et de soutien à la coopération entre Etats membres.

- Le second volet du Cybersecurity Act a pour but d'harmoniser à l'échelle européenne les modalités d'évaluation et les différents niveaux d'assurance de la certification. Cette certification atteste de la robustesse d'un produit réalisé par un évaluateur tiers tenant compte des évolutions technologiques. Plusieurs niveaux de certifications sont possibles et sont évalués par une autorité nationale désignée, l'ANSSI en France, ainsi que l'UE elle même via la Commission européenne et l'Agence de l'UE pour la cybersécurité qui permet l'élaboration d'un schéma, généralement retrouvé sous cette forme :



Ainsi, trois **niveaux** de certification sont proposés :

- le **niveau élémentaire** qui se fait par une autoévaluation du développeur et concerne des produits destinés au grand public,
- le **niveau substantiel** qui repose sur des tests de conformité effectué par un tiers de confiance accrédité (Conformity Assessment Body) qui intéresse généralement les produits dont le service est couvert par une assurance comme les Cloud,
- le **niveau élevé**, qui prend le nom de *"certification de Critères Communs"* en France. Il concerne des produits où il existe un risque d'attaque impliquant des compétences techniques comme par exemple les dispositifs médicaux connectés. Ce niveau est délivré par un organisme public qui sera chargé d'effectuer, en plus des tests de conformité, des test de pénétration pour tester sa capacité à être "hacké".

Ces certifications réduisent la fragmentation du marché et suppriment les obstacles réglementaires tout en renforçant la confiance.

En conclusion, l'UE est passé d'un soutien à la compétence à la lutte contre la fraude grâce à un encadrement des réseaux et systèmes d'information. Ensuite, l'UE lutte contre la fraude par le Cybersecurity *Act et le* RGPD *établissant une réelle protection pour tous les utilisateurs des réseaux et systèmes d'information ainsi que des produits qui les composent. Cependant, le* RGPD *et le* Cybersecurity Act *ont en réalité une limite considérable. Ils ont été adopté et publié alors que s'opérait une explosion de réseaux sociaux comme Tik Tok la création de nouvelle façon de se connecter comme la 5G, établissant alors un retard dès la publication de ces textes ne peuvent prendre en compte les nouvelles problématiques mises en lumière par ces évolutions.*

Il serait alors intéressant d'observer ce que le Digital Service Act (DSA)*, qui devrait être adopté le 15 décembre prochain pourrait apporter à ces limites. Le DSA est un ensemble de textes législatif de la Commission dont l'objectif est de mettre à jour le cadre juridique de l'UE en modernisant la direction sur le commerce électronique de 2000 et entre dans l'engagement de Ursula Von Der Leyen de l'élaboration d'une nouvelle législation sur les services numériques.*

RETOUR SUR LA CONVENTION DE BUDAPEST :

La Convention de Budapest est la première Convention à vocation Internationale sur la cybersécurité. Contraignante, elle est le premier pas vers l'harmonisation de l'encadrement des réseaux et systèmes d'information et plus largement le cyberespace. L'apport principal de cette Convention est considérable en ce qu'elle caractérise les cyberviolences et crimes commis dans ce cyberespace :

- Crime contre la confidentialité
- Infraction informatique
- Infraction sur le contenu
- Crime lié aux atteintes à la propriété intellectuelle
- Crime de diffusion de matériel raciste et xénophobe

Le groupe de travail sur la cyberintimidation et les autres formes de violences en ligne du Conseil de l'Europe va approfondir cette notion de cyberviolence et la définir un peu plus concrètement comme étant "l'utilisation des systèmes informatiques pour causer, faciliter ou menacer de causer à des personnes de la violence qui entraine ou est susceptible d'entrainer un préjudice ou des souffrances physiques, sexuelles, psychologiques ou économiques".

On se rend alors compte de ce phénomène d'amplification que créer Internet et son utilisation. Les violences dites "traditionnelles" y sont renouvelées sur Internet car la distance physique n'existe plus, les informations sont facilement stockées et rapidement accessible tout comme l'anonymat.

QU'EST CE QUE LA CYBERVIOLENCE?

La définition de la cyberviolence découle directement de cette notion de **cybercrimes** et **cyberintimidations**. Les plus touchés sont les femmes et les filles ce qui a une répercussion directe sur l'économie et la société européenne. Aujourd'hui et d'après un rapport sur la Cyberviolence à l'encontre des femmes et des filles de l'Institut européen pour l'égalité entre les Hommes et les Femmes (EIGE), une femme sur trois subira une forme de violence au cours de sa vie et une femme sur dix a déjà été victime d'une forme de cyberviolence dès l'âge de 15 ans.

Aucune conceptualisation de la **cyberviolence** n'a été effectué aujourd'hui, il n'y a pas non plus de définition législative de celle-ci à l'échelle de l'Union Européenne. Mais, le 11 février 2020, la **Cour Européenne des Droits de l'Homme** a permis une avancée substantielle en la matière car, à travers l'affaire **Buturaga contre Roumanie**, elle va définir la cyberviolence comme étant *"un aspect de la violence à l'encontre des femmes et des filles et peut se présenter sous diverses formes dont les violations informatiques de la vie privée, l'intrusion dans l'ordinateur, de la victime et la prise, le partage et la manipulation des données et des images, y compris des données intimes"*. Ce qui intéressant ici c'est que cette notion est rapprochée de celle d'infraction dans le sens d'une atteinte à l'intégrité et aux libertés de la personne, d'une atteinte sexuelle ou sexiste, atteinte qui soit répétée ou regroupée. On y trouve la diffamation, la vidéo-agression (une agression filmée et diffusée en direct), le cyberharcélement ou encore les messages malveillants.

Une attention particulière est donc apportée aux femmes qui permet une avancée féministe en la matière, et aux filles afin d'aller toujours plus loin dans la lutte contre la pédocriminalité et par extension la cyber-pédocriminalité.

Il est alors possible d'introduire la notion de **"viol à distance"**, notion très peu connue qui paraît un peu floue mais qui a été reconnu par la Suède ou encore la Belgique. La Suède a reconnu en 2017 un Homme coupable de viol à distance sur une trentaine d'enfants et a reconnu *"qu'un tel comportement revient au même que si l'auteur avait directement commis ces actes sur les victimes"*. La Belgique quant à elle a reconnu un homme coupable de viol à distance, ayant contraint une adolescente 15 ans à l'auto-pénétration.

Cependant, la France ne le reconnaît pas encore car définit le viol à l'article 222-23 du Code Pénal comme étant *"Tout acte de pénétration sexuelle, de quelque nature qu'il soit, commis sur la personne d'autrui ou sur la personne de l'auteur par violence, contrainte, menace ou surprise est un viol"*. Or, pour le viol à distance il n'y a pas de contact physique, l'auteur du viol n'est pas à l'origine de la pénétration sexuelle mais il l'a exigé, demandé ou payé quelqu'un d'autre pour le faire. Par exemple, Stephan Lambert, le 13 janvier 2020 a été condamnée à 5 ans de prison pour agression sexuelle à distance, le viol n'ayant malheureusement pas été reconnu. Un cas similaire a été observé à Grenoble où un homme mis en examen pour agression sexuelle à distance a finalement été condamné seulement pour "détention d'images pédopornographiques".

Ecrit par Guillemette Jahn,
Responsable Cybersécurité du Pôle Aerospace & Cybersecurity

Correctrices :

Anaëlle Le Lostec
Constance Alloy

Sitographie :

- hfile:///Users/GuillemetteJahn/Downloads/ti_pubpdf_mh0417543frn_pdfweb_20171026164001.pdf
- https://www.ssi.gouv.fr/uploads/2018/01/certification_securite_produits_visa_securite_anssi.pdf
- https://www.ssi.gouv.fr/administration/produits-certifies/cc/
- https://www.cnil.fr/fr/adoption-du-reglement-europeen-par-le-parlement-europeen-un-grand-pas-pour-la-protection-des-donnees
- hhttps://fr.wikipedia.org/wiki/Convention_sur_la_cybercriminalit%C3%A9
  ttps://cyberjustice.blog/index.php/2020/04/09/le-viol-a-distance-une-reconnaissance-est-elle-possible/

Suivez Def'INSEEC sur :

Def'INSEEC
Pole Aerospace & Cybersecurity