Revue de Droit Commercial Belge / Tijdschrift voor Belgisch Handelsrecht, 2019/8 - 1 octobre 2019

La fin de la saga *Skype*: les fournisseurs de services étrangers obligés de collaborer avec la justice belge en dépit des possibilités techniques et de leurs obligations en droit étranger

STRAFONDERZOEK - ONDERZOEKSDADEN

Gerechtelijk onderzoek - Onderzoeksdaden - Zoeken in informaticasysteem - Medewerkingsverplichting - Elektronische dienstverlener - Webmaildienst - Artikel 88*bis*, § 2 Sv. - Artikel 90*quater*, § 2 Sv. - Opsporing van verkeersgegevens - Onderscheppen van niet voor het publiek toegankelijke communicatie - Lokalisering van de medewerkingsverplichting - Economische activiteit op het Belgische grondgebied - Vrij verkeer van diensten - Wetsconflicten - Technische interceptiemogelijkheid

Een dienstverlener die een webmaildienst aanbiedt en die zijn economische activiteiten actief op consumenten in België richt, is verplicht mee te werken met de Belgische gerechtelijke autoriteiten, ongeacht de plaats waar die dienstverlener is gevestigd of waar de infrastructuur ligt die vereist is om gevolg te geven aan de vordering van de onderzoeksrechter. De artikelen 88bis, § 2 en 90quater, § 2 Sv. houden geen verplichting in om in België over een infrastructuur of andere fysieke aanwezigheid te beschikken, ondanks de inhoud van artikel 2, § 1 en 2 van het koninklijk besluit van 9 januari 2003.

De medewerkingsverplichting kan op Belgisch grondgebied worden gelokaliseerd aangezien er geen interventie van de Belgische gerechtelijke autoriteiten in het buitenland vereist is. Zodoende is de onderzoeksrechter er niet toe gehouden een rechtshulpverzoek te richten aan de Staat waar de dienstverlener zijn vestiging of infrastructuur heeft en is evenmin gebonden door de wetgeving van dat land. Het wetsconflict met het Luxemburgs recht maakt geen overmacht uit in hoofde van de dienstverlener die weigert mee te werken.

De dienstverlener wordt geacht zijn activiteiten dermate technisch te organiseren dat hij kan voldoen aan de medewerkingsverplichtingen naar Belgisch recht. In casu, had de dienstverlener zelfs geen intentie om mee te werken met het Belgische gerecht.

ENQUÊTE PÉNALE - MESURES D'ENQUÊTE

Instruction - Actes d'instruction - Recherche dans les systèmes informatiques - Obligation de collaboration - Fournisseur d'un service de communications électroniques - Messagerie électronique - Article 88*bis*, § 2, C.i.cr. - Article 90*quater*, § 2, C.i.cr. - Repérage de données de trafic - Interception de communications non accessibles au public - Localisation de l'obligation de collaboration - Activité économique sur le territoire belge - Libre prestation de services - Conflits de lois - Capacité technique d'interception

Un fournisseur d'un service de messagerie électronique dont l'activité économique s'adresse activement aux consommateurs en Belgique, a l'obligation de collaborer avec les autorités judiciaires belges, indépendamment du lieu où se trouve son siège social ou du lieu où se situe l'infrastructure requise pour donner suite à la demande du juge d'instruction. Une infrastructure ou autre présence physique en Belgique n'est pas requise par les articles 88bis, § 2 et 90quater, § 2, C.i.cr., malgré l'énoncé de l'article 2, § 1er et 2, de l'arrêté royal du 9 janvier 2003.

L'obligation de collaboration peut être localisée sur le territoire belge étant donné qu'elle ne requiert pas d'intervention des autorités judiciaires belges à l'étranger. Dès lors, le juge d'instruction n'est pas tenu d'adresser une demande d'entraide judiciaire à l'État où le siège ou l'infrastructure de ce fournisseur se trouve et n'est pas davantage lié par la législation de ce pays. Le conflit de lois avec le droit luxembourgeois ne constitue pas un cas de force majeure dans le chef du fournisseur qui refuse de collaborer.

Le fournisseur de services est tenu d'organiser ces activités de manière à pouvoir répondre aux obligations de collaboration imposées par le droit belge. En l'espèce, le fournisseur de services n'avait simplement pas l'intention de collaborer avec la justice belge.

La fin de la saga Skype: les fournisseurs de services étrangers obligés de collaborer avec la justice belge en dépit des possibilités techniques et de leurs obligations en droit étranger [2]

Vanessa Franssen [3] et Marine Corhay [4]

I. Introduction

Le 19 février 2019, la Cour de cassation a rendu son arrêt dans l'affaire *Skype*, attendu avec impatience par la communauté juridique et les acteurs économiques. Toutefois, l'arrêt offre très peu de réponses aux questions de taille qui se posent. En fait, un lecteur non initié aurait même beaucoup de mal à comprendre l'enjeu de l'affaire. L'objectif de ce commentaire est dès lors d'apporter, de manière succincte, un éclairage sur cet arrêt et les questions laissées en suspens, qui touchent à la thématique délicate mais fondamentale de la collaboration des fournisseurs de services autres que les traditionnels opérateurs et fournisseurs de services de télécommunications.

Dans un premier temps, nous esquisserons brièvement les faits et la procédure qui a précédé l'arrêt annoté. Ensuite, dans une seconde étape, nous expliquerons les questions soumises à la Cour de cassation, avant de procéder à une analyse critique de l'arrêt et de la législation nationale sur laquelle il se fonde. Nous clôturerons avec quelques mots de mise en perspective de cette jurisprudence, notamment en parallèle avec les actuelles négociations au niveau de l'Union européenne et du Conseil de l'Europe.

II. Faits et procédure devant les juridictions de fond

Les faits remontent à septembre 2012. Dans le cadre d'une enquête relative à une organisation criminelle, le juge d'instruction requiert que Skype Communications SARL (ci-après: Skype), d'un côté, produise des données de trafic relatives aux communications Skype d'un des suspects (art. 88*bis*, § 2, C.i.cr.) et, de l'autre, prête son concours technique à l'interception du contenu de ces communications (art. 90*quater*, § 2, C.i.cr.). Le suspect se trouve sur le territoire belge, plus particulièrement dans l'arrondissement judiciaire de Malines, et utilise le logiciel Skype pour communiquer avec ses comparses. Bien que Skype soit une entreprise étrangère sans infrastructure ni autre présence physique sur le territoire belge - l'entreprise a son siège social au Grand-Duché de Luxembourg -, le juge d'instruction décide de ne pas se servir des instruments relatifs à la coopération judiciaire en matière pénale (comme la convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne [5] et le traité d'extradition et d'entraide judiciaire en matière pénale entre le Royaume de Belgique, le Grand-Duché de Luxembourg et le Royaume des Pays-Bas du 27 juin 1962 [6]) mais de s'adresser directement à l'entreprise par simple courriel.

L'entreprise luxembourgeoise refuse toutefois de collaborer, arguant qu'elle peut uniquement fournir, sur une base volontaire, des données d'identification. Par contre, les données de trafic et l'assistance technique requises par le juge d'instruction exigent que les procédures d'entraide judiciaire soient suivies. Skype est, en effet, d'avis que les autorités judiciaires belges ne peuvent pas contraindre une entreprise étrangère qui n'a pas de présence physique sur le territoire belge sans le recours des autorités luxembourgeoises [7]. Sans l'intervention de ces dernières, Skype violerait la législation luxembourgeoise. De plus, elle invoque l'impossibilité technique d'intercepter le contenu des communications étant donné que le logiciel Skype est fondé sur une architecture *peer-to-peer*, décentralisée et distribuée, c'est-à-dire que les communications ne passent pas par un serveur central de l'entreprise Skype, mais se font directement entre les ordinateurs des utilisateurs [8].

Ce refus sera le début d'une longue procédure judiciaire, qui s'est terminée par l'arrêt de la Cour de cassation du 19 février 2019. En effet, le refus de collaboration étant incriminé par le Code d'instruction criminelle, le juge d'instruction en a informé le procureur du Roi qui, à son tour, a décidé, en mars 2014, d'engager des poursuites pénales contre Skype sur le fondement des articles 88*bis*, § 2 et 90*quater*, § 2, C.i.cr.

En première instance, Skype a été condamnée à une peine d'amende de 5.000 EUR (à majorer des décimes additionnels) par le tribunal correctionnel de Malines le 27 octobre 2016 [9]. Cette peine a été confirmée en degré d'appel par la cour d'appel d'Anvers par un arrêt du 15 novembre 2017 [10]. L'arrêt de la cour d'appel reprend largement le raisonnement du tribunal correctionnel.

Force est donc de constater qu'aucun des arguments avancés par la prévenue n'a pu convaincre les deux juridictions de fond. Il n'est pas possible, dans le cadre de ce commentaire, de détailler tous ces arguments; nous nous limiterons donc aux trois arguments principaux, à savoir le champ d'application territorial des articles 88*bis,* § 2 et 90*quater*, § 2, C.i.cr., le conflit de lois avec le droit luxembourgeois et l'impossibilité technique de collaborer.

Premièrement, les juridictions de fond estiment que Skype est visée par les obligations de collaboration prévues aux articles 88*bis*, § 2 et 90*quater*, § 2, C.i.cr., qui s'étendent à tout fournisseur d'un service de communications électroniques qui offre de manière ciblée des services sur le marché belge [11]. Peu importe l'endroit du siège social du fournisseur [12]. De plus,

l'exécution des réquisitions du juge d'instruction ne requiert pas de présence des autorités policières et judiciaires belges à l'étranger [13]. Tel a été décidé par la Cour de cassation dans l'affaire *Yahoo* en 2015 [14] et a, ensuite, été codifié par le législateur, notamment par la loi du 25 décembre 2016 [15], [16]. En conséquence, les autorités judiciaires belges peuvent se passer de la procédure d'entraide judiciaire et directement appliquer le droit belge à tous les fournisseurs de services étrangers qui sont virtuellement présents en Belgique. Sur le plan international, cette approche est loin de faire l'unanimité et risque de causer des *clashes* de souveraineté [17]. Beaucoup d'États (et d'auteurs) sont d'avis qu'il faut un autre critère de rattachement au territoire, notamment l'endroit du stockage des données ou le siège social du fournisseur de services [18]. Toutefois, il convient de noter qu'en ce qui concerne les données d'identification, l'approche belge est tout à fait en conformité avec la convention sur la cybercriminalité du Conseil de l'Europe. En son article 18, 1., b), cette convention donne effectivement la possibilité aux États parties d'émettre une injonction de production de données d'identification (ou « *des données relatives aux abonnés* », pour utiliser la terminologie de la convention) à l'égard d'un « *fournisseur de services offrant des prestations* ***sur le territoire*** *de la partie* » [19]. D'après une note d'orientation du Comité T-CY, la présence territoriale du fournisseur de services n'est pas forcément physique mais virtuelle [20]. La jurisprudence *Yahoo* était, dans ce sens [21], conforme à la convention, ou pour être plus correct, elle a contribué à l'adoption de la note d'orientation sur l'article 18 [22]. Toutefois, dans l'affaire *Skype*, le juge d'instruction belge va bien au-delà des pouvoirs accordés par l'article 18 de la convention sur la cybercriminalité.

Deuxièmement, tant le tribunal correctionnel que la cour d'appel ont écarté le moyen de défense basé sur le conflit de lois avec le droit luxembourgeois. Alors que Skype alléguait qu'elle ne pouvait pas collaborer avec la justice belge sans violer les règles luxembourgeoises relatives à la confidentialité des communications privées, en d'autres mots qu'elle était « *contrainte* » à ne pas respecter le droit pénal belge, les juges du fond ont jugé qu'il n'y avait même pas lieu d'analyser l'éventuelle contradiction entre le droit belge et le droit luxembourgeois puisque les communications ciblées avaient eu lieu sur le territoire belge et que l'entreprise devait prêter son concours au même endroit [23].

Troisièmement, les juridictions de fond ont rejeté l'argumentation de la défenderesse sur l'impossibilité technique de collaborer. D'après Skype, il lui était impossible d'intercepter les communications Skype sur le territoire belge, faute d'infrastructure en Belgique. Afin de pouvoir répondre aux réquisitions du juge d'instruction belge, elle aurait dû revoir de fond en comble la conception de son infrastructure et de son logiciel. Le tribunal correctionnel estime, toutefois, que l'entreprise Skype avait elle-même créé cette impossibilité technique puisqu'elle avait décidé d'organiser ses services, qu'elle offre notamment sur le marché belge, en utilisant une technologie *peer-to-peer* alors que la loi belge l'oblige à collaborer avec les autorités judiciaires pour collecter des données de trafic et de contenu relatives aux moyens de communications électroniques [24]. La cour d'appel renchérit en jugeant que le fait même de ne pas avoir conçu d'emblée ses installations techniques de manière à pouvoir répondre à ses obligations légales sur la base des articles 88*bis,* § 2 et 90*quater*, § 2, C.i.cr. constitue l'infraction qui est reprochée à l'entreprise Skype [25].

Insatisfaite de la décision des juges du fond, l'entreprise Skype décide de saisir la Cour de cassation.

III. Analyse de l'arrêt de la Cour de cassation

III.1. Moyens soulevés par la demanderesse

Devant la Cour de cassation, Skype invoque deux moyens comprenant plusieurs branches [26]. Les arguments de la demanderesse en cassation peuvent être résumés comme suit.

Premièrement [27], la demanderesse invoque la violation de l'article 56 du traité sur le fonctionnement de l'Union européenne [28] portant sur l'interdiction de restrictions à la libre prestation de services à l'intérieur de l'Union. D'après elle, les obligations de collaboration prévues aux articles 88*bis*, § 2 et 90*quater*, § 2, C.i.cr., lus conjointement avec l'article 2, § 1er et 2, de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques [29], impose à tout fournisseur d'un service de communications électroniques l'obligation d'avoir une infrastructure ou une autre forme de présence physique sur le territoire belge. En effet, même si la Cour de cassation dans l'affaire *Yahoo* a jugé que l'article 46*bis* C.i.cr. (concernant l'obligation de fournir des données d'identification) ne requiert pas une présence physique du fournisseur de services, l'article 2, § 1er-2 et § 4, de l'arrêté royal du 9 janvier 2003 prévoit que, pour satisfaire aux obligations de collaboration visées aux articles 46*bis*, § 2, 88*bis*, § 2 et 90*quater*, § 2, C.i.cr., chaque opérateur d'un réseau de communications électroniques et chaque fournisseur d'un service de communications électroniques doit établir, sur le territoire belge, une « Cellule de coordination de la Justice ». Cette dernière est composée d'une ou plusieurs personnes chargées d'assumer les tâches résultant des obligations de collaboration précitées et est disponible en permanence. Estimant que cette obligation d'établir une Cellule de coordination de la Justice constitue une restriction à la libre prestation des services au sein de l'Union européenne, Skype

demande à la Cour de cassation de poser une question préjudicielle à la Cour de justice de l'Union européenne sur la compatibilité de cette exigence du droit belge avec le droit de l'Union.

Dans un deuxième temps [30], Skype soulève que les mesures ordonnées par le juge d'instruction nécessitaient une requête d'entraide judiciaire et ne prennent pas en considération le droit luxembourgeois relatif à la protection de la vie privée des utilisateurs de ses services. L'absence d'une telle requête d'entraide judiciaire constitue, entre autres, une violation de l'article 18 de la convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne.

En dernier lieu [31], la demanderesse en cassation allègue une violation des articles 88*bis* et 90*quater* C.i.cr. ainsi que de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques [32], dans la mesure où la cour d'appel a décidé que Skype aurait dû prendre les mesures nécessaires pour pouvoir satisfaire à son obligation de collaboration découlant de l'article 88*bis* C.i.cr. L'entreprise estime qu'elle ne peut être tenue pénalement responsable que si la loi lui impose également une obligation de conserver les données demandées. Or, à son sens, une telle obligation de conservation de données n'existait pas pendant la période infractionnelle (septembre 2012-mars 2014). Cet argument est formulé de façon assez maladroite puisqu'il mélange deux choses: d'un côté, l'obligation pour le fournisseur de services de concevoir son infrastructure de manière à pouvoir répondre à ses obligations de collaboration imposées par le droit belge et, de l'autre, l'existence d'une obligation (générale) de conservation des données de trafic relatives aux communications électroniques. La première partie de l'argument revient sur l'argument déjà soulevé devant les juridictions de fond, sur l'étendue du concours technique du fournisseur de services, notamment en ce qui concerne l'interception du contenu de la communication; la seconde, par contre, touche à une autre problématique et se limite à l'obligation de produire des données de trafic.

III.2. Analyse critique des réponses fournies par la Cour de cassation

A. Impossibilité technique de collaborer

Au dernier moyen évoqué ci-dessus, la Cour de cassation répond de manière assez laconique que la condamnation de la demanderesse n'est pas fondée sur le motif invoqué, mais sur le motif que la demanderesse n'avait simplement pas l'intention de collaborer [33]. Ce manque d'intention est déduit du fait que l'entreprise Skype avait indiqué dans une de ses réponses aux autorités judiciaires belges qu'elle pouvait fournir tant des données d'identification que certaines données de trafic [34]. Autrement dit, lors de l'instruction, l'entreprise avait avoué pouvoir produire, au moins partiellement, les données requises sur la base de l'article 88*bis*, § 2, C.i.cr. Ainsi, elle s'était, en quelque sorte, tiré une balle dans le pied ce qui n'a pas facilité sa défense par la suite. Si elle avait produit toutes les données en sa possession et limité son refus aux données qu'elle n'avait pas et/ou à l'interception des communications Skype, soit la mesure la plus intrusive, son argument sur l'impossibilité technique de collaborer aurait sans doute été plus convaincant.

Ainsi, la Cour de cassation a laissé passer l'opportunité de se prononcer sur la question relative à la possibilité technique de collaborer. Ce choix est regrettable, d'autant plus qu'il s'agit d'une question absolument cruciale à l'ère où les communications électroniques sont de plus en plus cryptées [35], même par défaut, et ce, pour assurer le respect de la vie privée des utilisateurs mais, aussi, pour respecter les obligations de cybersécurité qui incombent aux entreprises actives sur le marché européen [36]. La procédure pénale belge oblige-t-elle les fournisseurs de services à doter leurs moyens de communications électroniques d'une capacité d'interception? Telle semble bien être la conséquence de l'arrêt de la cour d'appel d'Anvers (*supra*), même si certains auteurs ont critiqué, à juste titre, l'arrêt sur ce point [37] et que l'avocat général Decreus semble, lui aussi, d'un autre avis [38]. Toutefois, dans l'interprétation de la cour d'appel, le droit belge est-il compatible avec la législation européenne en matière de protection de données à caractère personnel et celle relative à la cybersécurité [39]? Est-il conforme à la convention sur la cybercriminalité [40]? Toutes ces questions, pourtant fondamentales, sont laissées en suspens, avec toute l'insécurité juridique qui en découle pour l'ensemble des fournisseurs de services actifs sur le marché belge.

Dans le même temps, l'affaire *Skype* est aussi une illustration de la nature fragile et incertaine de la coopération volontaire [41] (ou informelle [42]) des fournisseurs de services. Clairement, l'entreprise Skype avait la possibilité de fournir des données de trafic aux autorités judiciaires belges et il est même vraisemblable qu'elle en avait produit dans le passé [43]. Toutefois, confrontée à la demande d'intercepter le contenu des communications Skype, ce qui est une mesure plus intrusive encore que le transfert de données de trafic, l'entreprise a visiblement voulu changer sa pratique de collaboration. Ce revirement explique, bien sûr, la frustration du juge d'instruction en charge de l'enquête qui est à l'origine de l'affaire *Skype* et la volonté du procureur du Roi d'en faire un dossier exemplaire. Si, au moment des faits, un cadre juridique clair en matière de coopération directe avec les fournisseurs de services étrangers avait existé au niveau de l'Union européenne,

l'affaire *Skype* n'aurait sans doute pas vu le jour. La proposition « *e-evidence* » de la Commission européenne, publiée le 17 avril 2018, vise à créer un tel cadre juridique [44]; toutefois, elle s'applique uniquement aux données stockées et ne concerne pas l'interception de communications électroniques en temps réel [45]. Si cette proposition législative était adoptée, elle ne changerait donc pas l'actuelle situation en matière d'interception en temps réel. A noter, par ailleurs, que cette proposition n'aborde pas non plus de manière explicite la question du chiffrement [46]. Par contre, elle donne aux fournisseurs de services un moyen de défense lorsque ceux-ci ne disposent pas ou plus des données demandées par les autorités judiciaires [47].

B. Présence territoriale du fournisseur de services

Quant au moyen relatif à la restriction à la libre prestation de services, la Cour de cassation réussit à éviter assez facilement la question sur la discordance entre, d'une part, le vaste champ d'application territorial des articles 88*bis*, § 2 et 90*quater*, § 2, C.i.cr. et, d'autre part, l'exigence d'établir une Cellule de coordination de la Justice sur le territoire belge, prévue à l'article 2, § 1er et 2, de l'arrêté royal du 9 janvier 2003. En reprenant les motifs de l'arrêt de la cour d'appel, la Cour de cassation confirme que les dispositions légales du Code d'instruction criminelle n'imposent pas une obligation de disposer d'une infrastructure sur le territoire belge [48]. Quant à l'exigence de l'arrêté royal du 9 janvier 2003, la Cour considère que le grief fait à l'arrêt attaqué repose sur une lecture erronée puisque la condamnation par la cour d'appel est fondée uniquement sur les articles 88*bis*, § 2 et 90*quater*, § 2, C.i.cr. [49]. En conséquence, il n'est pas nécessaire de poser une question préjudicielle à la Cour de justice de l'Union européenne [50].

Pourtant, la contradiction entre le Code d'instruction criminelle et l'arrêté royal qui détermine les modalités de l'obligation de collaborer avec la justice belge est flagrante. Pour la comprendre, il faut remonter un peu dans le temps. A l'époque où l'arrêté royal fut adopté, le champ d'application personnel des articles 46*bis*, 88*bis* et 90*quater* C.i.cr. était plus limité qu'à l'heure actuelle. En effet, ces articles visaient uniquement les opérateurs d'un réseau de télécommunications et les fournisseurs d'un service de télécommunications. Il était à peine question des géants du web qui offrent à l'échelle mondiale des services Internet et de nouveaux outils de communication. C'est d'ailleurs en 2003 que le logiciel Skype fut lancé [51]. En d'autres mots, l'arrêté royal est écrit pour un autre type de fournisseur, les traditionnels opérateurs et fournisseurs de services de télécommunications, qui ont d'office une infrastructure sur le territoire. L'extension du champ d'application personnel des obligations de collaboration visées au Code d'instruction criminelle date de 2011, lorsque la Cour de cassation a jugé dans l'affaire *Yahoo* [52] que l'intention du législateur était d'inclure également d'autres fournisseurs de services [53]. Depuis la loi du 25 décembre 2016, cette interprétation est reflétée clairement dans le Code d'instruction criminelle [54]. En se référant à l'arrêté royal de 2003, Skype a tenté, en vain, de remettre en question l'interprétation retenue dans l'affaire *Yahoo*. Il n'en reste pas moins, qu'à l'heure actuelle, le contenu de l'article 2 de cet arrêté royal ne correspond plus au champ d'application personnel des articles au Code d'instruction criminelle et que cette discordance mériterait d'être adressée par le Roi.

C. Coopération directe et le sort des conflits de lois

Dans le seul sous-moyen de l'arrêt qui a été traduit en français [55], l'entreprise Skype dénonce la démarche choisie par le juge d'instruction. Au lieu d'appliquer les règles relatives à la coopération judiciaire en matière pénale, le juge a privilégié la voie de la coopération directe avec le fournisseur de services étranger, un acteur privé. Ce mode de coopération devient de plus en plus important en raison de l'utilisation répandue d'une grande variété de moyens de communication et de partage d'information via Internet [56]. Cette tendance croissante à recourir à la coopération directe au lieu de suivre la voie de l'entraide judiciaire, qui est plus lente et souvent inefficace [57], ne se manifeste pas seulement en Belgique, mais à l'échelle mondiale [58]. Toutefois, cette coopération avec les fournisseurs de services internet se situe souvent dans une zone grise faute de cadre juridique clair [59]. Comme indiqué *supra*, la Commission européenne veut offrir, avec sa proposition « *e-evidence* », une solution à ce problème. De même, au niveau du Conseil de l'Europe, on cherche à mieux réglementer la coopération directe en vue de l'obtention transfrontière des preuves numériques. C'est l'un des objectifs du futur second protocole additionnel à la convention sur la cybercriminalité [60].

L'une des questions sensibles dans le contexte de coopération directe est celle relative aux conflits de lois. Comment résoudre le conflit entre la loi de l'État du siège du fournisseur de services et celle de l'État qui requiert la collaboration du fournisseur de services? Cette question a également été soumise à la Cour de cassation dans cette affaire.

Pour y répondre, la Cour de cassation commence par réitérer sa jurisprudence *Yahoo* [61]. Les dispositions légales du Code d'instruction criminelle permettent au juge d'instruction de s'adresser directement au fournisseur de services étranger, « *indépendamment du lieu où cet opérateur ou ce fournisseur est établi ou du lieu où se situe l'infrastructure requise pour donner suite à la demande du juge d'instruction* » [62], pourvu que le fournisseur participe activement à la vie économique

en Belgique. A cet effet, une intervention des autorités judiciaires belges à l'étranger n'est pas requise et il « *n'est pas davantage lié par la législation [luxembourgeoise]* ». Comme l'arrêt attaqué explique, les communications ciblées par les réquisitions du juge d'instruction se situent en Belgique, et non pas au Luxembourg; dès lors, « *les prestations de services fournies par la demanderesse aux habitants belges relèvent du droit belge applicable et non du droit luxembourgeois* » [63]. En conséquence, « *l'infraction alléguée au droit luxembourgeois ne peut donc constituer un cas de force majeure dans le chef de la demanderesse* » [64]. En conséquence, la Cour conclut que la décision de la cour d'appel est légalement justifiée.

Si l'on peut questionner la localisation (exclusive) de l'obligation de collaboration en Belgique - d'autant plus parce qu'il s'agit de données de trafic et d'une interception du contenu de communications [65] -, il faut toutefois reconnaître que cette approche est également adoptée par d'autres pays [66]. Mais la conséquence que la Cour en tire - la simple non-application du droit luxembourgeois - est encore moins convaincante et pose question d'un point de vue du droit international.

Comme l'exprime l'article 2 de la charte des Nations Unies, les États sont souverains et la collaboration internationale est fondée sur le principe d'égalité souveraine. Ce principe suppose un respect mutuel de la souveraineté de l'autre. Il est donc tout à fait possible, voire logique que l'État du fournisseur de services impose des restrictions légales que ce dernier doit respecter, même s'il est confronté à des demandes légitimes d'un autre État, comme des demandes dans le cadre d'une enquête pénale concernant une infraction commise sur le territoire de cet État [67]. Ces restrictions légales créent un obstacle important à la coopération directe avec les fournisseurs de services. C'est notamment le cas pour la coopération entre autorités judiciaires en Europe et fournisseurs de services américains (parfois appelés les GAFAM [68]): le droit américain les empêche de produire, directement, le contenu de communications électroniques à des autorités judiciaires étrangères [69]. Ces fournisseurs peuvent uniquement produire de telles données dans le cadre d'une procédure d'entraide judiciaire. Or, afin de surmonter ce problème et de permettre une collaboration directe plus rapide et efficace entre les fournisseurs de services américains et les autorités judiciaires en Europe, l'Union européenne négocie en ce moment une convention avec les Etats-Unis sur base du CLOUD Act [70]. Au sein de l'Union européenne, c'est la proposition « *e-evidence* » qui permettra une coopération directe entre les fournisseurs de services d'un Etat membre (c.-à-d. l'Etat membre du siège du fournisseur ou celui où réside le représentant légal du fournisseur [71]) et les autorités judiciaires d'un autre Etat membre. Toutefois, il s'agit, dans les deux cas, d'initiatives législatives qui n'ont pas encore abouti.

Le droit belge actuel, qui instaure une coopération directe entre les autorités judiciaires belges et tout fournisseur de services étranger qui est actif sur le marché belge, sans base légale internationale [72], ne respecte donc pas la souveraineté de l'État du siège du fournisseur de services [73]. L'emprise du droit belge pourrait cependant être atténuée par la prise en compte des obligations légales qui incombent aux fournisseurs de services étrangers dans leur État d'origine. Une telle approche serait envisageable sur la base de l'article 70 du Code pénal, qui prévoit: « *Sauf en ce qui concerne les infractions définies dans le Livre II, Titre Ibis, il n'y a pas d'infraction, lorsque le fait était ordonné par la loi et commandé par l'autorité.* » Une obligation légale basée sur le droit du siège du fournisseur de services pourrait, à notre sens, constituer une cause de justification dans le chef du fournisseur, comme d'autres auteurs l'ont déjà suggéré [74].

Comme nous avons écrit ailleurs [75], en jouant cavalier seul, la Belgique met les fournisseurs de services Internet actifs sur le marché belge dans une situation inextricable: soit ils respectent leur obligation de collaboration en droit belge, soit ils violent la législation de l'État de leur siège social. Il est dès lors dommage que la Cour de cassation n'ait pas saisi l'opportunité d'atténuer les effets extraterritoriaux de l'actuelle législation.

Propos conclusifs

L'affaire *Skype* soulève des questions fondamentales relatives à la coopération transfrontière avec des fournisseurs de services étrangers, autres que les traditionnels fournisseurs de télécommunications. En raison de l'effacement des frontières dans le monde virtuel, les autorités judiciaires sont, quotidiennement, confrontées au besoin de pouvoir accéder, dans le cadre d'enquêtes pénales, à des données informatiques qui sont transmises, traitées ou stockées, souvent sous forme cryptée, par des fournisseurs de services établis à l'étranger. Malheureusement, la Cour de cassation apporte très peu de réponses à ces questions, et celles qu'elle donne sont peu satisfaisantes, tant pour les fournisseurs de services en question que pour les autres États concernés (en particulier, l'État du siège social). Cette jurisprudence est une excellente illustration des risques qu'entraîne une approche unilatérale à défaut d'un cadre juridique international. En fin de compte, c'est sans doute la principale leçon à tirer de cette affaire.

D'où notre appel aux décideurs politiques aux niveaux de l'Union européenne et du Conseil de l'Europe: afin d'éviter pire, il faut absolument trouver des solutions adéquates pour répondre aux besoins légitimes des autorités judiciaires. Compte tenu des faiblesses de l'entraide judiciaire à l'ère numérique [76], la coopération directe transfrontière entre autorités

judiciaires et acteurs privés est sans doute inéluctable. Le défi est donc d'élaborer des règles juridiques claires qui permettent, à la fois, de tenir compte de la souveraineté de l'État du siège social afin de limiter les conflits de lois et de garantir la protection des droits fondamentaux des individus concernés. Dans le même temps, il est essentiel que ces règles soient réalistes, praticables et plus efficaces que l'actuelle entraide judiciaire.

---

[1] Cette publication s'inscrit dans un projet de recherche de droit comparé financé par le F.R.S-FNRS (CDR J.0293.17) et l'ULiège, qui est consacré à la collaboration des fournisseurs de services dans le cadre des enquêtes pénales.

[2] Chargée de cours à l'ULiège, collaboratrice scientifique à la KU Leuven et membre du barreau de Bruxelles.

[3] Assistante à l'ULiège.

[4] Convention établie par le Conseil conformément à l'art. 34 du traité sur l'Union européenne, relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne du 29 mai 2000 (*J.O.C.E.*, C. 197, 12 juillet 2000, p. 3).

[5] Traité Benelux d'extradition et d'entraide judiciaire en matière pénale entre le Royaume de Belgique, le Grand-Duché de Luxembourg et le Royaume des Pays-Bas, adopté à Bruxelles le 27 juin 1692.

[6] Concernant la question de la compétence d'exécution de l'Etat belge à l'égard d'un fournisseur de services étranger sans présence physique sur le territoire, voy. K. De Schepper et F. Verbruggen, « Ontsnappen *space invaders* aan *onze pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van de medewerking door elektronische dienstverleners », *T. Strafr.*, 2013, p. 161.

[7] Toutefois, il paraît que l'architecture du logiciel a entretemps été modifiée, du moins en partie. Voy. p. ex. C. Bohic, « Skype n'abandonne pas tout à fait le P2P », *ITespresso*, 21 juillet 2016, disponible sur **www.itespresso.fr/skype-p2p-134873.html**.

[8] Corr. Anvers (div. Malines), 27 octobre 2016, n° de notice ME20.F1.105151-12, *Computerr.*, 2017, n° d'article 2017/6, note E. Valgaeren; *N.C.,* 2017, n° 1, p. 89.

[9] Anvers, 15 novembre 2017, n° de rôle 2016/CO/1006, *Computerr.*, 2018, n° d'article 2018/57, note C. Gysels.

[10] Pour déterminer si le marché belge a été ciblé, les facteurs suivants sont pris en compte: l'usage d'un nom de domaine belge, l'usage de la langue locale, la publicité faite en fonction de la localisation des utilisateurs, l'accessibilité des services pour les utilisateurs belges via notamment une boîte de réclamations et une rubrique FAQ. Ces facteurs ont été mis en avant par la Cour de cassation dans l'affaire *Yahoo*: Cass. 1er décembre 2015, P.13.2082.N. Pour une analyse, voy. V. Franssen et O. Leroux, « Recherche policière et judiciaire sur internet: analyse critique du nouveau cadre législatif belge », *in* V. Franssen et D. Flore (dirs.), *Société numérique et droit pénal. Belgique, France, Europe,* Bruxelles, Larcier-Bruylant, 2019, pp. 202-205.

[11] Corr. Anvers (div. Malines), 27 octobre 2016, n° de notice ME20.F1.105151-12, *Computerr.*, 2017, n° d'article 2017/6, note E. Valgaeren; *N.C.,* 2017, n° 1, p. 95-97, § 5.3; Anvers, 15 novembre 2017, n° de rôle 2016/CO/1006, *Computerr.*, 2018, n° d'article 2018/57, note C. Gysels, § 5.1.2.2.

[12] Corr. Anvers (div. Malines), 27 octobre 2016, n° de notice ME20.F1.105151-12, *Computerr.,* 2017, n° d'article 2017/6, note E. Valgaeren; *N.C.* 2017, n° 1, p. 96, § 5.3.3; Anvers, 15 novembre 2017, n° de rôle 2016/CO/1006, *Computerr.,* 2018, n° d'article 2018/57, note C. Gysels, § 5.1.2.3 *in fine*.

[13] Cass., 1er décembre 2015, P.13.2082.N. Pour une analyse, voy. R. Roex, « Belgische justitie kan rechtstreeks informatie opvragen van Amerikaanse techreuzen », *Juristenkrant*, 2015, n° 319, p. 5; K. De Schepper, « Doek valt over *Yahoo*-zaak », *Computerr.*, 2016, n° d'article 2016/35.

[14] Loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales (*M.B.*, 17 janvier 2017).

[15] Pour une analyse tant de l'arrêt que de la nouvelle législation, voy. V. Franssen, « The Belgian Internet Investigatory Powers Act. A Model to Pursue at European Level? », *EDPL*, 2017/4, pp. 538-540.

[16] Voy. p. ex., E. Valgaeren, « Yahoo en Skype: gelijke kappen? », *Computerr.*, 2017, n° d'article 2017/6: « *Dergelijk centripetaal rechtsmachtsbegrip is niet verenigbaar met de principes van een goed werkende internationale rechtsorde.* »

[17] Voy. p. ex., P. De Hert, C. Parlar et J. Thumfart, « Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland », *N.J.E.C.L.*, 2018, pp. 337-341; K. De Schepper et F. Verbruggen, *o.c.*, p. 161; F. Verbruggen, « 'Om af te sluiten, druk op Start': zesde rechter in Belgische *Yahoo*-zaak schaart zich achter eerste », *Computerr.*, 2014, n° d'article 2014/71, pp. 129-140.

[18] Nous soulignons.

[19] Comité de la convention sur la cybercriminalité (T-CY), *T-CY Guidance Note _10 Production orders for subscriber information (Article 18 Budapest Convention)*, Strasbourg, 1er mars 2017, p. 6, disponible sur www.rm.coe.int/16806f943e. Contrairement à l'article 18, 1., a), dont le champ d'application est limité aux personnes présentes sur le territoire de l'Etat partie, l'article 18, 1., b), peut être appliqué dans les cas où le fournisseur de services n'est ni légalement ni physiquement présent sur le territoire.

[20] A noter que la Cour de cassation s'est prononcée sur d'autres questions importantes dans cette affaire, lesquelles ne peuvent pas être élaborées dans ce commentaire. Pour une analyse plus approfondie, voy. R. Roex, *o.c.*, p. 5; K. De Schepper, *o.c.*

[21] En effet, la note d'orientation s'est inspirée des évolutions législatives et jurisprudentielles au niveau national, dont la jurisprudence *Yahoo*. Voy. Comité de la convention sur la cybercriminalité (T-CY), *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY*, Strasbourg, T-CY (2016)5 provisional, 16 septembre 2016, p. 21-22, § 63-64, disponible sur www.rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.

[22] Corr. Anvers (div. Malines), 27 octobre 2016, n° de notice ME20.F1.105151-12, *Computerr.*, 2017, n° d'article 2017/6, note E. Valgaeren; *N.C.* 2017, n° 1, p. 98, § 5.5.3; Anvers, 15 novembre 2017, n° de rôle 2016/CO/1006, *Computerr.,* 2018, n° d'article 2018/57, note C. Gysels, § 5.1.2.3.

[23] Corr. Anvers (div. Malines), 27 octobre 2016, n° de notice ME20.F1.105151-12, *Computerr.,* 2017, n° d'article 2017/6, note E. Valgaeren; *N.C.* 2017, n° 1, p. 97, § 5.5.2.

[24] Anvers, 15 novembre 2017, n° de rôle 2016/CO/1006, *Computerr.*, 2018, n° d'article 2018/57, note C. Gysels, § 5.1.2.3. Voy. aussi § 5.1.2.2 de cet arrêt.

[25] A noter que l'arrêt de la Cour de cassation, rendu en langue néerlandaise, n'a pas été traduit intégralement et que la traduction française ne comprend pas certains arguments. D'où le choix de publier la version intégrale de l'arrêt en néerlandais.

[26] Voy. not. les première et deuxième branches du premier moyen (§ 1-6 de l'arrêt) et la deuxième branche du deuxième moyen du pourvoi en cassation (§ 16-19 de l'arrêt).

[27] Traité sur le fonctionnement de l'Union européenne (version consolidée) (*J.O.U.E.,* C. 326, 26 octobre 2012, p. 47).

[28] *M.B.*, 10 février 2003.

[29] Voy. not. les troisième et quatrième branches du premier moyen du pourvoi en cassation (§ 7-11 de l'arrêt).

[30] Voy. not. la première branche du deuxième moyen du pourvoi en cassation (§ 14-15 de l'arrêt).

[31] *M.B.*, 20 juin 2005.

[32] Cass., 19 février 2019, P.17.229.N, § 15.

[33] Dans le jugement du tribunal correctionnel de Malines, il est question d'une « liste » de données qui peuvent être fournies sur une base volontaire (Corr. Anvers (div. Malines), 27 octobre 2016, n° de notice ME20.F1.105151-12, *Computerr.*, 2017, n° d'article 2017/6, note E. Valgaeren; *N.C.,* 2017, n° 1, p. 91, § 1.9.). La liste elle-même n'est pas reproduite dans le jugement, mais on peut déduire qu'elle contenait également certaines données de trafic.

[34] *Cf.* F. Verbruggen et S. Royer, « Veroordeling Skype niet verbroken, vele vragen blijven onbeantwoord », *R.W.*, 2018-2019, p. 1442.

[35] La Commission européenne travaille depuis un certain temps sur les défis posés par le chiffrement, mais fait preuve d'une grande réticence à légiférer, tellement la question est délicate. Jusqu'à présent, elle n'a proposé que des mesures pratiques pour répondre aux problèmes auxquels les autorités judiciaires sont confrontées. Voy. Commission européenne, Onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 608, Bruxelles, 18 octobre 2017, pp. 8-10, disponible sur www.ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-608-F1-FR-MAIN-PART-1.PDF.

[36] C. Gysels, note sous Anvers, 15 novembre 2017, *Computerr.*, 2018, n° d'article 2018/57; C. Conings, *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Anvers, Intersentia, 2017, pp. 287-288.

[37] L'avocat général Decreus ne semble, en effet, pas favorable à l'interprétation de la cour d'appel, bien qu'il aborde la question sous l'angle du champ d'application personnel: « *Men dient van een wetgever in een rechtsstaat te veronderstellen dat hij geen strafrechtelijk gesanctioneerde medewerkingsplicht oplegt aan personen die niet aan de plicht kunnen voldoen. Zo niet dreigt pure willekeur, hetzij bij het oordeel dat een persoon in een concrete zaak niet over bepaalde gegevens beschikte of vanuit technisch oogpunt niet beter had kunnen meewerken en daardoor toch niet kan veroordeeld worden, hetzij bij het oordeel dat een persoon in een concrete zaak over gegevens had kunnen beschikken of zich zo had kunnen organiseren dat hij beter kon meewerken en daardoor wel kan veroordeeld worden.* » Cass., 19 février 2019, P.17.229.N, Concl. Av. gén. L. Decreus, p. 12.

[38] En vertu du droit de l'Union européenne, les fournisseurs d'un service de communications électroniques sont tenus de garantir la sécurité de leurs réseaux et services. De manière plus générale, toute personne responsable du traitement de données à caractère personnel est obligée de garantir une sécurité appropriée de ces données, y compris par le biais du chiffrement. Voy., entre autres, art. 4, 1., de la directive n° 2002/58/CE du Parlement et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (*J.O.C.E.*, L. 201, 31 juillet 2002, p. 37); art. 40, 1., de la directive (UE) n° 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le Code des communications électroniques européen (refonte) (*J.O.U.E.*, L. 321, 17 décembre 2018, p. 36); art. 5, 1., f) et art. 32 du règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive n° 95/46/CE (règlement général sur la protection des données) (*J.O.U.E.*, L. 199, 4 mai 2016, p. 1); art. 16, 1., directive (UE) n° 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (*J.O.U.E.*, L. 194, 19 juillet 2016, p. 1).

[39] De toute évidence, la convention ne contraint pas les fournisseurs de services à créer une capacité d'interception. En matière d'interception des données relatives au contenu, l'art. 21, 1., b), de la convention prévoit que chaque partie peut obliger un fournisseur de services à prêter aux autorités compétentes son concours et son assistance pour collecter ou pour enregistrer ces données, « *dans le cadre de ses capacités techniques* ». L'art. 20, 1., b), de la convention prévoit une obligation similaire en matière de collecte en temps réel des données relatives au trafic est même plus explicite: « *dans le cadre de ses capacités techniques* ***existantes*** » (nous soulignons). Voy. modification *infra*, notes 46, 51 et 64 pour uniformiser l'approche.

[40] C.-à-d. une coopération qui ne repose pas sur une obligation légale. A l'heure actuelle, la coopération volontaire représente un grand pourcentage de cas, surtout en ce qui concerne les géants du web américains. Certains fournisseurs acceptent des demandes directes de données non relatives au contenu. Voy. considérant 8, Commission européenne, proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, 2018/0108(COD), Strasbourg, 17 avril 2018 (ci-après: la proposition de règlement *e-evidence*). Voy. aussi P. de Hert, C. Parlar et J. Thumfart, *o.c.*, pp. 328-329.

[41] A.M. Osula, « Remote search and seizure in domestic criminal procedure: Estonian case study », *International Journal of Law and Information Technology*, 2016, pp. 344-345.

[42] C'est du moins ce qui ressort de discussions avec les autorités judiciaires.

[43] Cette proposition consiste, en réalité, en deux textes intrinsèquement liés: d'un côté, une proposition de règlement *e-evidence* et, de l'autre, une proposition de directive. Commission européenne, proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de collecte de preuves en matière pénale, 2018/0107 (COD), Strasbourg, 17 avril 2018 (ci-après: la proposition de directive *e-evidence*).

[44] Considérant 19 de la proposition de règlement *e-evidence*. A noter que, pour une interception en temps réel, un juge d'instruction belge peut émettre, depuis le 22 mai 2017, une décision d'enquête européenne. Au moment des faits, cet instrument n'était toutefois pas encore d'application. Voy. art. 38 et 39 de la loi relative à la décision d'enquête européenne en matière pénale (*M.B.*, 23 mai 2017). Cette loi transpose la directive n° 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale (*J.O.U.E.*, L. 130, 1 mai 2014, p. 1).

[45] Voy. V. Franssen, « The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement », *European Law Blog*, 12 octobre 2018, disponible sur www.europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/.

[46] Art. 9, 4., de la proposition de règlement *e-evidence*: « *Si le destinataire ne peut pas respecter son obligation* ***pour cause de force majeure ou d'impossibilité de fait qui ne lui est pas imputable*** *ou, le cas échéant, qui n'est pas imputable au fournisseur de services, notamment parce que la personne dont les données sont requises n'est pas leur client, ou* ***que les données ont été supprimées avant la réception de l'EPOC,*** *le destinataire en informe l'autorité d'émission mentionnée dans l'EPOC sans retard injustifié, en expliquant les raisons au moyen du formulaire figurant à l'annexe III. Si les conditions pertinentes sont remplies, l'autorité d'émission retire l'EPOC* » (nous soulignons).

[47] Cass., 19 février 2019, P.17.229.N, § 2.

[48] Cass., 19 février 2019, P.17.229.N, § 3 et 18.

[49] Cass., 19 février 2019, P.17.229.N, § 4 et 19. Voy. aussi F. Verbruggen et S. Royer, *o.c.*, p. 1442.

[50] Voy. www.en.wikipedia.org/wiki/Skype (dernier accès le 23 octobre 2019).

[51] Cass., 18 janvier 2011, N.C., 2011, p. 76, § 6: « *'Le fournisseur d'un service de télécommunications électroniques' au sens de l'article 46bis du Code d'instruction criminelle n'est pas uniquement l'opérateur belge au sens de la loi du 13 juin 2005 relative aux communications électroniques, mais quiconque dispense des services de communications électroniques, comme notamment la transmission de données de communication.*

L'obligation de concours prévue par l'article 46bis du Code d'instruction criminelle ne se limite, dès lors, pas aux opérateurs d'un réseau de communications électroniques ou aux fournisseurs d'un service de communications électroniques qui sont aussi opérateurs au sens de la loi du 13 juin 2005 ou qui dispensent leurs services de communications électroniques qu'au moyen de leur propre infrastructure. Cette obligation existe aussi dans le chef de celui qui fournit un service consistant entièrement ou principalement dans la transmission de signaux par la voie des réseaux de communications électroniques ***et la personne qui fournit un service consistant à autoriser ses clients à obtenir ou recevoir ou diffuser des informations au moyen d'un réseau électronique*** *peut aussi être un fournisseur d'un service de communications électroniques* » (nous soulignons). Pour une analyse de cette jurisprudence, voy. V. Franssen et O. Leroux, *o.c.*, pp. 197-199 et les références y mentionnées.

[52] V. Franssen et O. Leroux, *o.c.*, pp. 197-198. A noter aussi que l'avocat général Decreus, dans ses conclusions, revient amplement sur l'interprétation du terme « fournisseur d'un service de télécommunication/communication électronique »: Cass., 19 février 2019, P.17.229.N, Concl. Av. gén. L. Decreus, pp. 6 et s. Pour une analyse, voy. C. Gysels, « De medewerkingsplicht bij het onderzoek onbeslecht », *Computerr.*, 2019, n° d'article 2019/138.

[53] Pour une analyse de la codification apportée par la loi du 25 décembre 2016, voy. V. Franssen et O. Leroux, *o.c.*, pp. 199-202.

[54] Cass., 19 février 2019, P.17.229.N, § 7-10.

[55] Pour une analyse des enjeux que pose l'utilisation des nouvelles technologies d'information et de communication, voy. V. Franssen, A. Berrendorf et M. Corhay, « La collecte transfrontière de preuves numériques en matière pénale. Enjeux et perspectives européennes », *eR.I.D.P.*, 2019, n° article A-02, pp. 1-4, disponible sur www.penal.org/sites/default/files/Franssen%20collecte%20transfrontiere_0.pdf.

[56] P. De Hert, C. Parlar et J. Thumfart, *o.c.*, p. 328 et les références y mentionnées; S. Tosza, « Cross-border gathering electronic evidence: mutual legal assistance, its shortcomings and remedies", *in* V. Franssen et D. Flore (dirs.), *Société numérique et droit pénal. Belgique, France, Europe,* Bruxelles, Larcier-Bruylant, 2019, p. 269; K. De Schepper et F. Verbruggen, *o.c.*, p. 164.

[57] Voy. p. ex., P. De Hert, C. Parlar et J. Thumfart, *o.c.*, pp. 328 et 337-340; S. Carrera, G. González Fuster, E. Guild et V. Mitsilegas, *Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights*, Bruxelles, Centre for European Policy Studies, 2015, pp. 6 et 9-14.

[58] Le cadre juridique actuel est fragmenté et complexe, ce qui est problématique tant pour les Etats que pour les fournisseurs de services. Proposition de règlement *e-evidence*, p. 8. Voy. aussi P. De Hert, C. Parlar et J. Thumfart, *o.c.*, p. 329.

[59] Comite de la convention sur la cybercriminalité (T-CY), Mandat pour la préparation d'un projet de 2e protocole à la convention sur la cybercriminalité, Strasbourg, 9 juin 2017, disponible sur www.rm.coe.int/mandat-pour-la-preparation-d-un-projet-de-2e-protocole-a-la-convention/168072380f. Pour l'état actuel de ces négociations, voy. www.coe.int/en/web/cybercrime/t-cy-drafting-group (consulté le 1er décembre 2019). Voy. aussi V. Franssen, A. Berrendorf et M. Corhay, *o.c.*, pp. 13-14.

[60] Cass., 1er décembre 2015, P.13.2082, § 5 et 9.

[61] Cass., 19 février 2019, P.17.229.N, § 9.

[62] Cass., 19 février 2019, P.17.229.N, § 10.

[63] *Ibid.*

[64] F. Verbruggen, *o.c.*, pp. 129-140; F. Verbruggen et S. Royer, *o.c.*, p. 1442: « *Door het bevel, het verplichte medewerkingsgedrag van het bedrijf én het weigeringsmisdrijf* ***kunstmatig exclusief*** *op het Belgische grondgebied te lokaliseren, vindt België dat het volledig autonoom kan handelen* » (nous soulignons). Voy. aussi E. Valgaeren, *o.c.*: « *De nochtans onmiskenbare extraneïteitsfactor, nl. dat een tap wel degelijk een technische interventie vereist die allicht in Luxemburg (of in technische centra elders ter wereld) doch noodzakelijkerwijze buiten België diende te gebeuren, wordt zo gemakkelijkheidshalve weggeredeneerd.* » Et encore dans le même sens: C. Gysels, note sous Anvers, 15 novembre 2017, *Computerr.*, 2018, n° d'article 2018/57: « *(…) een wezenlijk verschil tussen het geven van retroactieve inlichtingen over een bestaand e-mailaccount en het verlenen van technische medewerking aan een registratie- en afluistermaatregel in de toekomst. (…) De tapmaatregel zelf zal dan ook naar alle waarschijnlijkheid niet eens succesvol bij Skype zelf kunnen gebeuren, maar eerder in datacenters of systemen, gelegen buiten Luxemburg, of derde partijen. Door de technische medewerking van Skype aan een tapmaatregel louter te herleiden tot het ter beschikking stellen van informatie, data en/of technische ondersteuning in België, gaat men volkomen voorbij aan de technologische werkelijkheid* ».

[65] P. ex., au Royaume-Uni, la législation prévoit une obligation de collaboration pour les opérateurs de télécommunications (*telecommunications operators*), qui offrent ou mettent à disposition leurs services à des personnes au Royaume-Uni, dans le cadre de la mise en oeuvre de mandats d'interception de télécommunications. Il faut lire conjointement les sections 43 (1), (2) et 261 (10) (a) de l'Investigatory Powers Act 2016, Chapter 25, disponible sur www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

[66] A ce sujet, Verbruggen observe, à juste titre, que le droit de l'Union européenne opère une distinction fondamentale entre l'Etat où l'entreprise est établie et celui où elle fournit des services. Voy. F. Verbruggen, *o.c.*, pp. 129-140.

[67] Google, Apple, Facebook, Amazon, Microsoft.

[68] Electronic Communications Privacy Act of 1986, texte intégral disponible sur www.law.cornell.edu/topn/electronic_communications_privacy_act_of_1986.

[69] Consolidated Appropriation Act of 2018, Division V - Clarifying Lawful Overseas Use of Data Act (*Pub. L.* n°. 115-141, 132 Stat. 348 (2018)). Pour une analyse succincte, voy. J. Daskal, « Unpacking the *CLOUD Act* », *eucrim*, 2018/4, pp. 220-225.

[70] Art. 7, 1., de la proposition de règlement *e-evidence*; art. 3 de la proposition de directive *e-evidence*.

[71] Si l'art. 18 de la convention sur la cybercriminalité permet une telle coopération directe pour les données d'identification (*supra*), il n'existe pas de base légale internationale pour les données de trafic et les données de contenu en ce moment.

[72] *Cf.* F. Verbruggen, *o.c.*, pp. 129-140.

[73] Voy. p. ex., J. Vanheule et F. Verbruggen, « Hink-stap-struikel naar het recht van morgen: daderschap, deelneming en (een beetje) bestraffing in het nieuwe Boek 1 van het Strafwetboek », *in Straf- en strafprocesrecht*, Themis, Vol. 110, Bruges, die Keure, 2019, p. 4, note 12.

[74] V. Franssen, *o.c.*, pp. 540-542.

[75] Voy., entre autres, S. Tosza, « Cross-border Gathering of Electronic Evidence: Mutual Legal Assistance, Its Shortcomings and Remedies », in V. Franssen et D. Flore (dirs.), *Société numérique et droit pénal. Belgique, France, Europe,* Bruxelles, Larcier-Bruylant, 2019, pp. 271-273.