_swissprivacy.law

Législation européenne – application extraterritoriale et souveraineté suisse

Nicolas Sacroug et Marc Løebekken, le 16 juin 2023

Depuis quelques années, de nombreuses juridictions tentent de réguler Internet et les services l'utilisant. Qu'il s'agisse de problématiques de concurrence, de poursuite pénale, de protection des consommateurs ou autres, les propositions ne manquent pas et trouvent un intérêt grandissant. L'Union européenne se distingue particulièrement par ses législations qui, le plus souvent, étendent leur champ d'application au-delà de ses frontières et peuvent avoir des répercussions en Suisse.

Introduction

Depuis quelques années, de nombreuses juridictions tentent de réguler Internet et les services l'utilisant. Qu'il s'agisse de problématiques de concurrence, de poursuite pénale, de protection des consommateurs ou autres, les propositions ne manquent pas et trouvent un intérêt grandissant.

L'Union européenne fait office de figure de proue avec l'entrée en vigueur du RGPD en 2018. Le RGPD n'a pas seulement introduit de nombreux principes relatifs aux données personnelles des utilisateurs et à leur traitement, il a également innové s'agissant de sa portée, en présentant un champ d'application extraterritorial extrêmement large (art. 3 par. 2 RGPD). En voulant protéger les données des citoyens européens, le législateur communautaire a rendu applicable le RGPD à tout fournisseur offrant des services sur le territoire européen indépendamment de sa localisation.

Depuis lors, de nombreuses lois, notamment européennes, empruntent un mécanisme d'extraterritorialité similaire, à l'instar du *Digital Service Act* (DSA), entré en vigueur en novembre 2022 ou encore du projet de règlement e-evidence, encore en discussion auprès des instances européennes. Le premier vise en substance à réguler l'activité des fournisseurs de services en ligne, tandis que le second a pour but de faciliter l'investigation de cyberdélits par les autorités de poursuite pénale.

Légiférer en la matière paraît raisonnable, tant il apparaît que les cyberinfractions peuvent aujourd'hui être commises d'un côté du globe et leurs résultats apparaître de l'autre.

Cependant, l'approche du parlement européen ne vient pas sans son lot de dangers. Un acte normatif visant à déployer ses effets sur le territoire d'un autre État peut en effet poser de nombreuses questions sur son applicabilité et son *enforcement*, particulièrement dans le cas où le droit national de ce second État comporterait des dispositions difficilement conciliables avec l'acte normatif en question.

Législation européenne et souveraineté suisse

L'un des défis principaux que présentent des textes comme le DSA ou le règlement e-evidence pour les entreprises suisses tient à l'introduction d'obligations de communication directe avec les autorités de poursuite pénale étrangères, sans passer par les procédures d'entraide internationale. Or l'art. 271 CP interdit généralement un tel comportement.

La Suisse a en effet adhéré à de nombreux textes bi- ou multilatéraux d'entraide internationale. L'on peut citer par exemple les Conventions de la Haye de 1965 et 1970 ou la Convention du 23 novembre 2001 sur la Cybercriminalité (Convention de Budapest, CCC). Ces textes ont en commun de prévoir une procédure par laquelle toute demande d'entraide judiciaire est relayée par les autorités étatiques désignées des deux États concernés. Celles-ci s'assurent de la légalité de la demande, de sa forme et de son bien-fondé. Les actes d'instruction, le cas échéant, sont ordonnés par l'État requis selon son droit national. Aucun contact n'a lieu entre l'autorité de l'État requérant et le fournisseur sis dans l'État requis auquel les actes d'instruction sont ordonnés.

Le mécanisme du DSA semble relativement peu problématique à cet égard. Ses art. 9 et 10 prévoient l'obligation, pour certaines catégories de fournisseurs de services, d'informer l'autorité requérante de « la suite éventuelle donnée à (une) injonction » d'agir contre du contenu illicite, respectivement de fournir des informations (art. 9 al. 1 et 10 par. 1 DSA). L'art. 18 prévoit quant à lui une obligation des fournisseurs de notifier les soupçons de commission de certaines infractions pénales aux autorités compétentes. Ces obligations concernent les autorités de n'importe que État membre de l'UE ainsi que tout fournisseur soumis, peu importe sa localisation ou celles des données concernées. Les paragraphes 6 de ces deux articles précisent que « les conditions et exigences établies dans le présent article sont sans préjudice du droit national applicable en matière de procédure civile et de procédure pénale ». Les let. h et i de l'art. 2, réglant le champ d'application de la loi, expriment déjà le fait que le DSA s'entend sans préjudice du « droit de l'Union dans le domaine de la coopération judiciaire en matière civile », respectivement pénale.

Il ne s'agit ainsi peut-être pas ici de contourner les mécanismes d'entraide, mais de

permettre une meilleure communication entre les autorités concernées et les fournisseurs de services, en obligeant ces derniers ne serait-ce qu'à répondre aux injonctions qu'ils reçoivent. Les considérants 31 à 36 apportent quelques indications à cet égard en précisant que le DSA ne fait pas office de base juridique pour l'émission de ces injonctions (consid. 31), mais que cela relève du droit national ou de l'Union (consid. 32). Il est également précisé que « lorsque ces législations prévoient, dans le cadre de procédures pénales ou civiles, des conditions supplémentaires à celles prévues dans le présent règlement ou incompatibles avec celles-ci en ce qui concerne les injonctions (…), les conditions prévues dans le présent règlement pourraient ne pas s'appliquer ou être adaptées » (consid. 34).

La situation est quelque peu différente avec le projet de règlement e-evidence. Celui-ci vise justement à contourner les canaux d'entraide internationale afin d'accélérer la collecte de preuve de cyberinfractions (consid. 8). Si le texte est approuvé dans sa teneur actuelle, les autorités européennes pourront adresser une requête directement à un fournisseur de services électroniques indépendamment de sa localisation pour autant qu'il offre ses services dans l'UE (art. 1 par. 1). Le compromis actuel permettrait en effet à une autorité européenne investiguant un cas cyber d'envoyer un ordre de production de données à un fournisseur situé hors du territoire de l'UE, c'est-à-dire notamment en Suisse.

Or une telle obligation semble difficilement compatible avec la législation suisse. L'art. 271 CP punit d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire quiconque « sans y être autorisé, aura procédé sur le territoire suisse pour un État étranger à des actes qui relèvent des pouvoirs publics ». Cet article vise à protéger la souveraineté nationale et à s'assurer du fait que seules les autorités étatiques suisses procèdent à des actes officiels sur le territoire helvétique (ATF 148 IV 66). Cet article vise justement à éviter le contournement des procédures d'entraide internationale et à protéger « le monopole du pouvoir étatique et la souveraineté suisse » (ATF 148 IV 66). Selon la jurisprudence, l'élément central quant à l'acte incriminé est celui de son caractère officiel et non la fonction de son auteur (ATF 114 IV 128).

Ce que cela signifie pour les entreprises suisses

Les entreprises suisses sembleraient devoir moins s'inquiéter des obligations du DSA que de celles de l'e-evidence, en ce qui concerne la fourniture de renseignements à l'étranger. Leur application reste cependant encore à confirmer.

Ainsi, tout entreprise ou indépendant suisse a intérêt à s'assurer des limites légales de ses communications avec les autorités ou tribunaux étrangers.

La voie de l'entraide judiciaire doit être empruntée pour toute communication de renseignements relative à une procédure pénale ou civile instruite à l'étranger. Cela signifie concrètement qu'un fournisseur de services suisse ne peut répondre qu'aux ordres de production de renseignements relayés par la police ou les ministères publics suisses (notamment par le biais des art. 265 et 273 CPP) ou par le Service Surveillance de la correspondance par poste et télécommunication (Service SCPT) pour le volet pénal ou par les tribunaux civils compétents.

Du point de vue des fournisseurs de services, de tels mécanismes permettent généralement de s'assurer de la légalité et de la légitimité des demandes reçues ainsi que de centraliser les voies de communication. Les risques de transmission de données à une autorité inexistante (*phishing*) s'en trouvent également limitées.

L'imposition aux fournisseurs de services par l'Union européenne d'obligations de transmission directe de données aux autorités étrangères présente ainsi de nombreux risques et soulève de nombreuses questions. Quelle option choisir entre accepter la demande étrangère, transmettre les informations et risquer une sanction de droit suisse ou refuser de collaborer et être condamné en Europe ? Une telle sanction serait-elle reconnue et applicable en Suisse ?

Même le RGPD, règlement pourtant en vigueur depuis quelques années et jouissant d'une grande visibilité, ne peut nous venir en aide : il n'existe, à notre connaissance, au moment de rédaction du présent article, aucun cas d'*enforcement* de celui-ci en Suisse. La manière dont les tribunaux interpréteront et appliqueront cette loi en Suisse ou la reconnaissance des sanctions prononcées à l'étranger sur sa base restent encore incertaines.

La Confédération non plus ne semble pas vouloir répondre à ces questions. Le Groupe de coordination interdépartemental de la Confédération « Politique numérique UE » (le Groupe de Coordination), agissant sous la coordination de l'OFCOM et du DFAE a récemment publié son document d'analyse « La Suisse et la stratégie numérique de l'Union européenne », présentant les différentes propositions de législation européenne concernant le numérique, et leur impact (potentiel) sur la Suisse. Ce document d'analyse se concentre principalement sur l'accès au marché européen par les entreprises suisses et reste muet sur les obligations de transmission de données et leur applicabilité au vu de l'art. 271 CP. Le Groupe de Coordination arrive à la conclusion qu'aucune action immédiate n'est nécessaire.

Pour l'instant, la Confédération adopte une position de « *wait and see* », estimant qu'il est difficile, voire impossible, d'évaluer les risques posés par une législation avant son entrée en

vigueur. Or une telle incertitude n'est nullement souhaitable pour les entités suisses potentiellement impactées par ces règlements. L'insécurité juridique à laquelle les fournisseurs de services font face en ce moment est grande et les questions de principe auxquelles ils tentent de répondre nombreuses. Il devrait pourtant revenir à la Confédération d'apporter ces réponses.

Cette position passive n'a pas manqué d'attirer l'attention du milieu politique (Motion 21.3676, Bellaiche), dont une de ses représentantes a déposé une motion forçant le Conseil fédéral à définir sa position sur ces réglementations et à participer activement aux négociations européennes. Le Conseil national a récemment adopté cette motion, à l'encontre de la recommandation du Conseil fédéral, qui s'était contenté d'affirmer sa position.

Conclusion

Le dossier n'est donc largement pas encore clos. De nombreux projets spécifiques au domaine informatique circulent actuellement au sein des autorités législatives européennes, la plupart visant à s'appliquer de manière extraterritoriale. Tout porte à croire que l'UE ne compte pas diminuer la cadence ni changer de stratégie. L'insécurité juridique n'est pas prête d'être résolue par elle-même.

La sollicitation des entreprises suisses par les autorités de poursuite étrangères risque fortement d'augmenter ces prochaines années. Il est donc important de se rappeler des limites de la coopération pouvant être offerte, particulièrement au vu de l'art. 271 CP et de limiter autant que possible les contacts pouvant éventuellement être considérés comme constitutifs d'un acte officiel pénalement répréhensible.

Si l'administration fédérale, et particulièrement l'OFJ, ne s'est pas encore prononcée sur ces points et sur leur interprétation, elle peut en revanche prêter assistance dans des cas concrets. En attendant des éclaircissements, nous ne pouvons qu'encourager les entreprises et particuliers suisses à jouer la prudence et à demander de l'aide aux autorités fédérales le cas échéant.

Proposition de citation : Nicolas Sacroug / Marc L□ebekken, Législation européenne – application extraterritoriale et souveraineté suisse, 16 juin 2023 *in* www.swissprivacy.law/233