Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Office fédéral de la justice OFJ

24 octobre 2023

Rapport sur le projet e-evidence de l'UE

BJ-D-FFB23401/87

Table des matières

1 Contexte

L'ère du numérique ne transforme pas seulement les différents aspects de nos existences, mais également les méthodes auxquelles ont recours les criminels dans le cadre de leurs activités. Ainsi, afin d'assurer l'efficacité de la poursuite pénale, il est indispensable que les autorités compétentes en la matière de même que les autres organismes qui participent à la lutte contre le crime s'adaptent à ces nouveaux développements. Cela comprend également l'adoption de **bases légales adéquates** pour une lutte efficace contre le crime.

Pour accompagner les défis inhérents à la révolution numérique sur le plan de la lutte contre le crime, de nouveaux instruments ont été et sont en train d'être négociés au niveau international. Ainsi, le Deuxième Protocole additionnel à la convention du Conseil de l'Europe sur la cybercriminalité a été adopté le 17 novembre 2021 afin de renforcer la coopération et de faciliter la transmission de preuves électroniques. En outre, une convention sur la cybercriminalité est en cours de négociation dans le cadre des Nations Unies. En parallèle, les États développent également leur législation en la matière : en novembre 2018, les États-Unis ont adopté le **Clarifying Lawful Overseas Use of Data Act (CLOUD Act)**, qui a pour but de permettre aux autorités de poursuite pénale d'accéder plus facilement aux données stockées à l'étranger. En raison de l'importance pratique du CLOUD Act, l'OFJ l'a examiné à la lumière du droit suisse et a publié le 17 septembre 2021 un rapport consacré à ce thème (rapport sur le US CLOUD Act (loi Cloud) ci-après : rapport CLOUD Act).

Face à ces développements, l'Union européenne (UE) n'est pas en reste et a adopté une nouvelle réglementation sur les preuves électroniques, appelé **paquet e-evidence**. Celui-ci s'inscrit dans le contexte des attentats de Bruxelles de 2016 : deux jours après les attentats, les ministres de la justice et de l'intérieur des États membres de l'UE ont exigé un meilleur accès aux preuves électroniques. Suite à cela, le Conseil de l'UE avait souligné à son tour le rôle essentiel revêtu par un accès efficace aux preuves électroniques afin de mieux lutter contre la criminalité grave et le terrorisme. Le 17 avril 2018, la Commission a présenté sa proposition de directive et de règlement en matière de preuves électroniques.

Le 13 juin 2023, le Parlement européen a adopté le paquet législatif e-evidence, qui a ensuite été approuvé par le Conseil de l'UE le 27 juin 2023, puis **publié au Journal officiel de l'UE le 28 juillet 2023**. Son but est de créer un cadre législatif cohérent dans le droit de l'UE afin de régler l'accès aux preuves électroniques et d'accélérer leur obtention. La nouvelle réglementation permet en particulier aux autorités de poursuite pénale des États membres de l'UE d'adresser directement leurs demandes de preuves aux fournisseurs de services dans d'autres États membres (« injonctions de production ») ou d'exiger la conservation de données pendant une période allant jusqu'à 60 jours afin d'éviter que les données concernées ne soient détruites ou perdues (« injonctions de conservation »). Elle crée ainsi un mécanisme alternatif à la procédure d'entraide judiciaire toujours applicable aujourd'hui.

La nouvelle réglementation pourrait également avoir des effets importants pour la Suisse, car les fournisseurs de services qui y sont établis et fournissent leurs services dans l'UE seront soumis en présence de certaines conditions aux nouveaux textes de loi. On pense par exemple aux services de communication comme Threema ou Protonmail. Toutefois, ces règles pourraient concerner également d'autres services numériques proposés par les entreprises suisses.

En complément au rapport CLOUD Act, le présent rapport vise à expliquer le contenu du paquet e-evidence de l'UE, à analyser les aspects de droit comparé et à mettre en évidence les conséquences et défis pour la Suisse de même que les différences par rapport au CLOUD Act américain. Enfin, le rapport explore les options qui s'offrent à la Suisse pour agir en la matière.

2 Contenu du paquet e-evidence

2.1 Condensé

Le paquet e-evidence se compose d'une directive, qui expose les principes essentiels du projet, et d'un règlement qui contient des dispositions détaillées.

La **directive**[1] oblige les fournisseurs qui proposent certains services numériques dans l'UE à désigner un établissement ou un représentant légal sur le territoire de l'UE auxquels les autorités des États membres peuvent adresser leurs injonctions de production et de conservation.

Le **règlement**[2] institue l'injonction européenne de production et l'injonction européenne de conservation. Il définit les conditions de l'obligation des fournisseurs de services qui proposent des services dans l'UE d'avoir un établissement sur le territoire de l'UE ou d'y désigner un représentant légal. Il règle en outre les conditions auxquelles les autorités (de poursuite pénale) compétentes d'un État membre de l'UE peuvent ordonner directement aux fournisseurs de services de produire ou de conserver des données.

Le règlement n'est pas applicable aux procédures engagées en vue de fournir une entraide judiciaire à un autre État membre de l'UE ou à un État tiers.

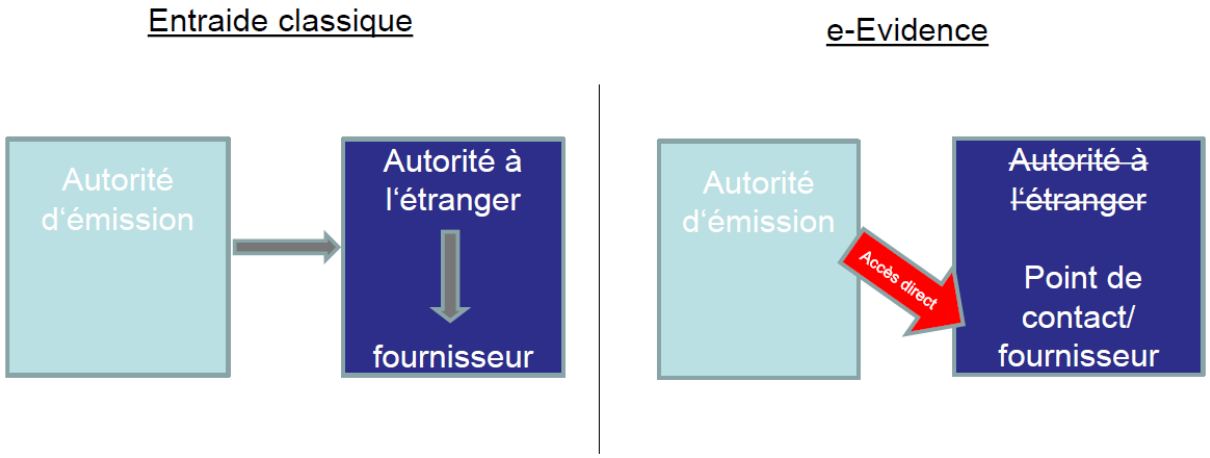

Illustration : fonctionnement du système e-evidence en comparaison avec la procédure classique d'entraide judiciaire

2.2 Bases légales au sein de l'UE

Comme mentionné, le paquet e-evidence repose sur deux instruments différents, un règlement et une directive. Bien que ces deux instruments se complètent, ils ne reposent toutefois pas sur les mêmes bases légales sur le plan du droit primaire.

La directive se fonde sur les art. 53 et 63 du traité sur le fonctionnement de l'Union européenne (TFUE). Ces deux articles figurent au titre IV du TFUE qui traite de la libre circulation des personnes, des services et des capitaux. En revanche, le règlement se base sur l'art. 82, par. 1 TFUE relatif à la reconnaissance mutuelle des jugements et au renforcement de la coopération

[1] DIRECTIVE (UE) 2023/1544 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales, JO L 191/181

[2] RÈGLEMENT (UE) 2023/1543 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale, JO L 191/118

judiciaire en matière pénale. Cet article figure au titre V du TFUE, qui traite de l'espace de liberté, de sécurité et de justice.

Bien que cette différence de base légale primaire puisse sembler anodine au premier abord, elle a des conséquences en pratique, car le Danemark et l'Irlande ont décidé de ne pas participer au titre V du TFUE. Alors que le Danemark a une option de retrait complète et ne prend part à aucun des instruments adoptés sur la base de ce titre, l'Irlande a une option de retrait partielle, ce qui signifie qu'elle peut au besoin participer à certaines initiatives de l'espace de liberté, de sécurité et de justice.

Pour le paquet e-evidence, cela signifie que le Danemark et l'Irlande doivent tous deux mettre en œuvre la directive mais non le règlement, et que contrairement au Danemark, l'Irlande a la possibilité de mettre en œuvre le règlement si elle le souhaite. Cependant, le règlement reprend plusieurs instruments de l'UE qui reposent sur le titre V, auxquels l'Irlande n'est pas forcément partie, raison pour laquelle une mise en œuvre du règlement e-evidence par cet État pourrait s'avérer compliquée en pratique[3].

2.3 Champ d'application

2.3.1 Fournisseurs de services

En premier lieu se pose la question des fournisseurs de services précisément visés par le paquet législatif.

Le règlement prévoit d'abord une condition de nature très générale selon laquelle on entend par fournisseur de services **toute personne physique ou morale qui fournit une ou plusieurs des catégories de services visés par le règlement**. Les services proposés exclusivement en dehors de l'UE n'entrent pas dans le champ d'application du règlement, même lorsque le fournisseur concerné possède un établissement dans l'UE. La question des fournisseurs concernés par le règlement dépend donc du type de prestations proposées par ceux-ci.

2.3.2 Services concernés

Ensuite se pose la question **des services** concernés concrètement par le règlement. Ceux-ci sont énumérés à l'art. 3, par. 3 du règlement. Il s'agit des services faisant partie des catégories suivantes.

2.3.2.1 Services de communications électroniques

Le règlement renvoie la définition fournie à l'art. 2, par. 4 de la directive (UE) 2018/1972 établissant le code des communications électroniques européen. Aux termes de cette directive, « est un service de communications électroniques », le service fourni normalement contre rémunération via des réseaux de communications électroniques qui comprend les types de services suivants :

- les services d'accès à Internet (en Suisse, par exemple **Swisscom, UPC-Sunrise**, etc.) ;
- les services de communications interpersonnelles, ce par quoi il y a lieu de comprendre, conformément à l'art. 2, par. 5 de la directive (UE) 2018/1972, un service normalement fourni contre rémunération qui permet l'échange direct d'informations entre un nombre fini de personnes, par lequel les personnes qui

[3] L'Irlande semble avoir décidé d'appliquer le règlement, voir le ch. 3 ci-dessous.

amorcent la communication ou y participent en déterminent le ou les destinataires (en Suisse, par exemple **Prontonmail ou Threema**) ;
- les services consistant entièrement ou principalement en la transmission de signaux tels que les services de transmission utilisés pour la fourniture de services de machine à machine et pour la radiodiffusion (par ex. **fournisseurs de blogs, services de vidéo à la demande ou réseaux sociaux**).

2.3.2.2 Services d'attribution de noms de domaine et de numérotation IP

Cela comprend les fournisseurs d'adresses IP, les services du bureau d'enregistrement de noms de domaine, ainsi que les fournisseurs qui proposent des services de proxy en lien avec des noms de domaine (en Suisse, par exemple **Switch, ProtonVPN**, etc.).

2.3.2.3 Autres services qui permettent à leurs utilisateurs de communiquer entre eux ou de stocker ou de traiter d'une autre manière des données pour le compte des utilisateurs auxquels le service est fourni

Sur ce point, le règlement renvoie à la description figurant à l'art. 1, par. 1, let. b de la directive UE 2015/1535, selon lequel le terme « service » désigne tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services[4].

Cette description quelque peu compliquée et difficile à comprendre est illustrée par des exemples à l'annexe I de ladite directive qui la rendent plus compréhensible. Selon cette annexe, les services suivants **ne sont pas couverts** par la liste figurant à l'art. 1, par. 1, let. b :

- services prestés en présence physique du prestataire et du destinataire, même s'ils impliquent l'utilisation de dispositifs électroniques (examen ou traitement dans un cabinet de médecin au moyen d'équipements électroniques, mais en présence physique du patient ; consultation d'un catalogue électronique dans un magasin en présence physique du client ; réservation d'un billet d'avion via un réseau d'ordinateurs dans une agence de voyage en présence physique du client) **(a contrario, les services suivants couverts seraient : les magasins en ligne, fournisseurs de réservations en ligne de billets d'avion, etc.) ;**
- mise à disposition de jeux électroniques dans une galerie en présence physique de l'utilisateur **(a contrario, les services couverts seraient : les fournisseurs de jeux en ligne) ;**
- services dont le contenu est matériel même s'ils impliquent l'utilisation de dispositifs électroniques (distribution automatique de billets de banque ou de billets de train ; accès aux réseaux routiers, parkings payants, etc., même si à l'entrée et/ou à la sortie des dispositifs électroniques interviennent pour contrôler l'accès et/ou assurer le paiement correct **(a contrario, les services couverts seraient : les applications de parkings, application CFF, etc.) ;**
- services « off-line » (distribution de CD-ROM ou de logiciels sur disquette) **(a contrario, les services couverts seraient : les services en ligne) ;**
- services qui ne sont pas fournis au moyen de systèmes électroniques de stockage et de traitement de données (services de téléphonie vocale ; services de télécopieur/télex ; services prestés par téléphonie vocale ou télécopieur ; consultation d'un médecin par téléphone/télécopieur ; consultation d'un avocat par téléphone/télécopieur ; marketing direct par téléphone/télécopieur) **(a contrario, les services couverts seraient : les conseils fournis en ligne dans les domaines concernés) ;**

[4] Le terme « service presté à distance » désigne un service fourni sans que les parties soient simultanément présentes ; le terme « service presté par voie électronique » désigne un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques ; le terme « service presté à la demande individuelle d'un destinataire de services » désigne un service fourni par transmission de données sur demande individuelle.

- services non fournis à la demande individuelle d'un destinataire de services, mais par l'envoi de données sans appel individuel et destinés à la réception simultanée d'un nombre illimité de destinataires (transmission « point à multi-point ») (services de radiodiffusion télévisuelle (y compris la quasi-vidéo à la demande) ; services de radiodiffusion sonore ; télétexte (télévisuel)) **(a contrario, les services couverts seraient : les services fournis à la demande individuelle, par ex. les journaux en ligne ou les podcasts).**

Par ailleurs, l'art. 3, par. 4 précise ce qu'il faut comprendre par **« proposer / fournir des services dans l'Union »** : le fournisseur de services doit permettre aux personnes physiques ou morales dans un État membre d'utiliser les services **énumérés au par. 3)** et avoir un lien substantiel, fondé sur des critères factuels spécifiques, avec un État membre. Un tel lien substantiel est réputé exister :

- lorsque le fournisseur de services dispose d'un établissement dans l'UE ; ou
- lorsqu'il existe un nombre significatif d'utilisateurs dans un ou plusieurs États membres ; ou
- lorsqu'il existe un ciblage des activités sur un ou plusieurs États membres (par ex. du fait de l'usage d'une langue ou d'une devise généralement utilisée dans cet État membre ou du fait de la possibilité de commander chez lui des biens ou des services). Le ciblage des activités sur un État membre pourrait également être constaté sur la base de la disponibilité d'une application dans la boutique d'applications nationale correspondante, de la diffusion de publicité locale ou de publicité dans la langue généralement utilisée dans cet État membre, ou de la gestion des relations avec la clientèle, comme la fourniture d'un service à la clientèle dans la langue généralement utilisée dans cet État membre[5].

Par contre, la seule accessibilité dans l'UE d'un site Internet d'un fournisseur de services ou la publication d'une simple adresse e-mail ou d'autres données de contact du fournisseur de services ne suffisent pas à elles seules pour déterminer si un fournisseur de services propose des services dans l'Union[6].

→ Lorsqu'un fournisseur propose un service couvert par l'art. 3, par. 3 et qu'il existe un lien substantiel avec l'UE, il doit soit avoir un établissement dans l'UE, soit y désigner un représentant légal.

2.3.3 Données concernées

Le paquet e-evidence couvre uniquement les données qui concernent des services proposés dans l'UE. Si tel est le cas, l'emplacement des données ne joue aucun rôle (elles peuvent également se situer en dehors du territoire de l'UE).

2.3.3.1 Données relatives aux abonnés, au trafic et au contenu

Sont concernées les données relatives aux abonnés[7], les données demandées à la seule fin d'identifier l'utilisateur[8], les données relatives au trafic (données secondaires)[9] et les données

[5] Cf. considérant (30) du préambule du règlement.

[6] Cf. considérant (29) du préambule du règlement.

[7] Les données relatives aux abonnés recouvrent d'une part toutes les données qui permettent de déterminer l'identité d'un abonné ou d'un client, telles que le nom, la date de naissance, l'adresse, les données de facturation et de paiement, le numéro de téléphone ou l'adresse électronique fournis, et d'autre part les données relatives au type de service et à sa durée.

[8] Elles comprennent les adresses IP et, si nécessaire, les ports sources et les horodatages correspondants, à savoir la date et l'heure.

[9] Les données relatives au trafic recouvrent par exemple la source et la destination d'un message ou d'un autre type d'interaction, l'emplacement du dispositif, la date, l'heure, la durée, la taille, le routage, le format, le protocole utilisé et le type de compression, et d'autres métadonnées de communications électroniques et des données, autres que les données relatives aux abonnés, relatives au début et à la fin d'une session d'accès d'un utilisateur à un service, telles que la date et l'heure d'utilisation, la connexion et la déconnexion du service.

relatives au contenu[10] (art. 3, par. 9 à 12 du règlement). En revanche, la surveillance en temps réel, à savoir par exemple l'écoute téléphonique en temps réel, n'est pas possible.

2.3.3.2 Données protégées par le secret professionnel, par des immunités ou par des privilèges

Le règlement contient en outre des dispositions expressément consacrées aux données qui sont protégées par le secret professionnel, en vertu du droit de l'État d'émission (cf. art. 5, par. 9 s. du règlement). Lorsque ces données sont stockées ou traitées d'une autre manière par un fournisseur de services en tant que partie d'une infrastructure fournie à des professionnels soumis au secret professionnel, dans le cadre de leur activité professionnelle[11], une injonction européenne de production visant à obtenir des données relatives au trafic ou des données relatives au contenu ne peut être émise que :

- lorsque le professionnel soumis au secret professionnel réside dans l'État d'émission ;
- lorsque le fait de s'adresser à ce professionnel soumis au secret professionnel pourrait nuire à l'enquête ; ou
- lorsque le secret professionnel a été levé conformément au droit applicable.

Si l'autorité d'émission a des raisons de croire que les données relatives au trafic ou les données relatives au contenu demandées sont protégées par des immunités ou des privilèges accordés, en vertu du droit de l'État chargé de la mise en œuvre, ou qu'elles sont protégées, en vertu de la liberté de la presse ou de la liberté d'expression, elle peut demander des éclaircissements à l'État chargé de la mise en œuvre avant d'émettre l'injonction européenne de production.

2.4 Production et stockage des données : l'injonction européenne de production et l'injonction européenne de conservation

2.4.1 Injonction européenne de production (art. 5 du règlement)

L'injonction européenne de production permet à l'autorité compétente d'un État membre de demander directement à des fournisseurs de services établis ou représentés dans un autre État membre la production de données qui relèvent du champ d'application du paquet e-evidence.

L'injonction européenne de production doit être **nécessaire et proportionnée**. De plus, elle ne peut être émise que si une injonction similaire aurait pu être émise dans les mêmes conditions dans le cadre d'une procédure nationale similaire (art. 5, par. 2 du règlement).

En outre, une injonction de production est admise uniquement pour des **infractions pénales passibles d'une certaine quotité de peine**, étant précisé que cette quotité dépend du type de données :

- les données relatives aux abonnés et les données demandées à la seule fin d'identifier l'utilisateur peuvent être demandées pour toutes les infractions pénales ainsi que pour l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté d'au moins quatre mois ;
- les données relatives au trafic et au contenu peuvent être demandées pour les infractions pénales punissables dans l'État d'émission d'une peine privative de liberté d'une durée d'au moins trois ans, pour certaines infractions énumérées dans des directives séparées (fraude et contrefaçon de moyens de paiement, abus

[10] Les données relatives au contenu recouvrent toutes les données dans un format numérique telles que du texte, de la voix, des vidéos, des images et du son, autres que les données relatives aux abonnés ou les données relatives au trafic.

[11] On pense par exemple au système de gestion électronique des dossiers d'une étude d'avocats.

sexuels et exploitation sexuelle d'enfants, pédopornographie, atteintes à des systèmes d'information) et pour l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté d'au moins quatre mois.

2.4.2 Injonction européenne de conservation (art. 6 du règlement)

L'injonction européenne de conservation permet à l'autorité compétente d'un État membre d'obliger un fournisseur de services établi ou représenté dans un autre État membre de conserver des données spécifiques pendant une certaine période.

Elle doit être **nécessaire et proportionnée** afin d'empêcher le retrait, la suppression ou la modification de données en vue d'une demande d'entraide judiciaire, d'une décision d'enquête européenne[12] ou d'une injonction européenne de production.

Elle peut être est émise pour toutes les infractions pénales lorsqu'elle aurait pu être émise dans les mêmes conditions dans le cadre d'une procédure nationale similaire, et pour l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté d'au moins quatre mois.

2.4.3 Autorité d'émission

Le règlement détermine également les autorités des États membres autorisées à demander des données, à savoir à émettre une injonction européenne de production ou de conservation et à l'adresser directement au fournisseur de services.

L'autorité de l'État d'émission qui peut exiger directement la production des données dépend du type de données concernées (art. 4 du règlement).

Les *données relatives aux abonnés* peuvent être demandées par un juge, une juridiction, un juge d'instruction ou un procureur compétents dans l'affaire concernée. En outre, toute autre autorité compétente désignée par son droit national comme compétente pour ordonner la collecte de telles données, conformément au droit national, peut demander la production de ces données, lorsque l'injonction est validée par un juge, une juridiction, un juge d'instruction ou un procureur dans l'État d'émission.

La production des *données relatives au trafic et au contenu* est plus restreinte. Elle peut être demandée par un juge, une juridiction ou un juge d'instruction compétents dans l'affaire concernée, ou par toute autre autorité compétente en vertu du droit de l'État d'émission, à condition que l'injonction ait été examinée et approuvée (validation) par un juge, une juridiction ou un juge d'instruction. Contrairement aux données relatives aux abonnés, les données relatives au trafic et au contenu ne peuvent pas être demandées par un procureur de manière autonome. Le Ministère public pourrait toutefois formuler une proposition en ce sens (cf. art. 4, par. 2, let. b du règlement) qui devrait ensuite être approuvée par une autorité judiciaire.

S'agissant de la conservation des données, une distinction est opérée en fonction du type de données : la conservation des données peut être demandée par un juge, une juridiction, un juge d'instruction ou un procureur ou par toute autre autorité compétente définie par l'État d'émission, conformément au droit national. Dans ce cas, un juge, une juridiction, un juge d'instruction ou un procureur doit déclarer l'injonction valable (validation).

[12] La décision d'enquête européenne est une décision judiciaire émise par une autorité judiciaire d'un État membre de l'UE qui vise à faire exécuter des mesures d'enquête en vue de recueillir des preuves en matière pénale dans un autre État membre.

2.4.4 Destinataires des injonctions

Les destinataires des injonctions de production sont les fournisseurs de services. Le principe est que l'injonction de production est adressée directement au fournisseur de services agissant en qualité de responsable du traitement (art. 5, par. 6 du règlement). La qualité de responsable du traitement est définie à l'art. 4, par. 7 du règlement général sur la protection des données de l'UE (RGPD)[13] :

> *Le « responsable du traitement » est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.*

L'injonction de production peut, à titre exceptionnel, être adressée directement au fournisseur de services qui stocke ou traite d'une autre manière les données pour le compte du responsable du traitement (sous-traitant)[14], lorsque le responsable du traitement ne peut pas être identifié malgré des efforts raisonnables de la part de l'autorité d'émission ou lorsque le fait de s'adresser à lui pourrait nuire à l'enquête. Dans ce cas, le sous-traitant est tenu d'informer le responsable du traitement de la production des données, sauf si l'autorité d'émission lui a demandé de s'en abstenir, afin de ne pas entraver la procédure pénale concernée (art. 5, par. 7 du règlement)[15].

L'art. 5, par. 8 du règlement contient en outre une limitation importante concernant les données qui sont stockées ou traitées d'une autre manière par un fournisseur de services pour une autorité publique. Pour ce type de données, une injonction de production ne peut être émise que si l'autorité publique est située dans l'État d'émission.

Tant les injonctions de production que les injonctions de conservation doivent être adressées directement à l'établissement ou au représentant légal désigné par le fournisseur de services concerné. Lorsque l'établissement ou le représentant légal désigné ne réagit pas, l'injonction de production peut être adressée dans les cas d'urgence à tout autre établissement ou représentant légal du fournisseur de services dans l'UE. Dans certains cas, l'État chargé de la mise en œuvre doit également être informé (cf. ch. 1.4.5).

2.4.5 Notification à l'État chargé de la mise en œuvre

Chaque État membre peut désigner une ou plusieurs autorités centrales compétentes pour la transmission administrative de certificats, d'injonctions ou de notifications, pour la réception de données et de notifications et pour la transmission de correspondance officielle.

Lorsque l'autorité d'émission requiert la production de données relatives au trafic ou au contenu, elle est tenue d'adresser une notification à l'autorité compétente de l'État chargé de la mise en œuvre (c'est-à-dire de l'État dans lequel le fournisseur de services est établi ou dans lequel il a désigné son représentant légal), en lui transmettant dans le même temps l'injonction de production (art. 8, par. 1 du règlement). Dans certains cas, une telle notification n'est pas nécessaire, notamment lorsque l'État d'émission a des motifs raisonnables de croire que l'infraction a été commise, est en train d'être commise ou est susceptible d'être commise sur

[13] Les considérants et dispositions du règlement renvoient directement aux dispositions pertinentes du RGPD et de la directive relative à la protection des données à caractère personnel.

[14] Aux termes de l'art. 4, par. 8, du RGPD, le « sous-traitant » est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

[15] Dans ce domaine, le règlement e-evidence l'emporte sur le RGPD, qui prévoit un devoir d'information du responsable du traitement envers le sous-traitant.

son territoire, et que la personne dont les données sont demandées y est domiciliée (« critère du domicile »).

L'autorité chargée de la mise en œuvre dispose ensuite d'un délai de dix jours pour évaluer l'injonction et, en cas d'urgence, de 96 heures au plus (art. 12 du règlement ; cf. ci-dessous). Les motifs de refus sont énumérés de manière exhaustive dans le règlement (cf. ch. 2.4.6.). Lorsque l'autorité chargée de la mise en œuvre ne soulève aucune objection, le fournisseur de services est tenu de produire les données, ce qui signifie qu'une approbation active de la part de l'État chargé de la mise en œuvre n'est pas nécessaire (cf. ch. 2.4.7.).

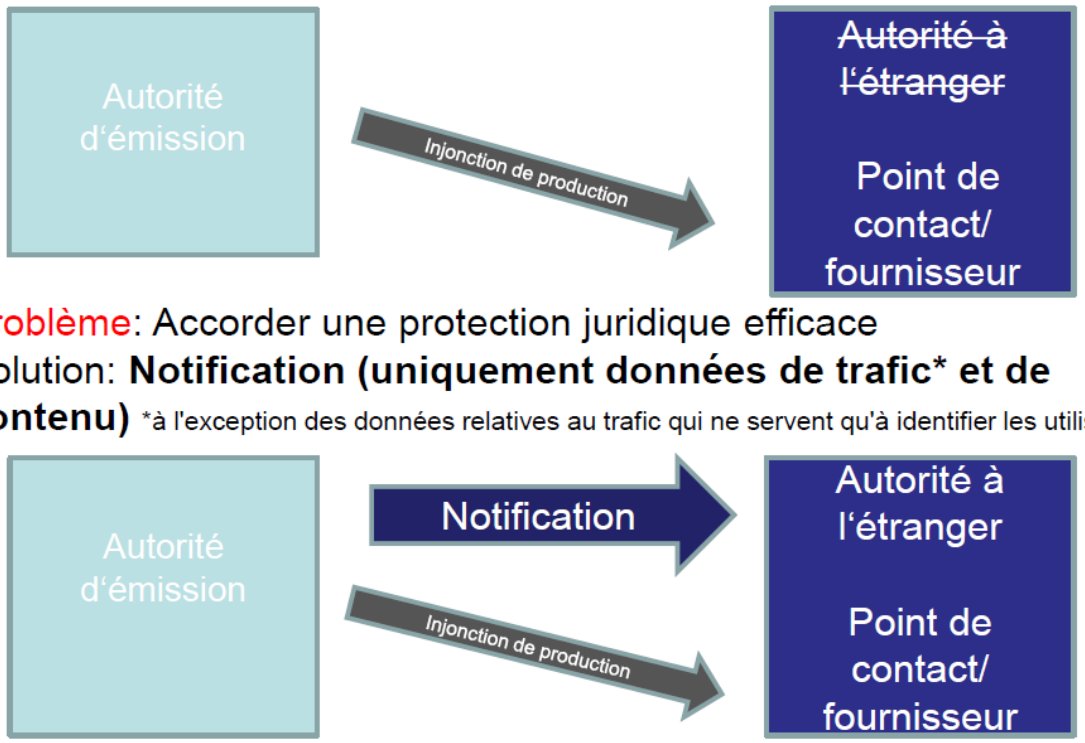

Illustration : implication de l'État chargé de l'exécution au moyen d'une « notification »

L'obligation de notifier a des limites strictes. Elle ne s'applique pas aux injonctions de conservation, ni aux injonctions de production de données relatives aux abonnés ou au trafic qui servent uniquement à identifier l'utilisateur. Cela peut avoir des conséquences graves si l'injonction vise l'identification de sources journalistiques ou de lanceurs d'alerte. Il incombe le cas échéant au fournisseur de services de faire valoir une violation de la liberté de la presse ou de la liberté d'expression, car l'État chargé de la mise en œuvre n'est pas informé (cf. ch. 2.4.6). Si le fournisseur de services n'invoque pas une telle violation, il peut arriver que des données soient produites alors qu'elles ne l'auraient pas été en raison de cette violation par la voie de la procédure d'entraide judiciaire. Le « critère du domicile » est également problématique, car son examen est laissé au seul pouvoir d'appréciation des autorités de poursuite pénale de l'État d'émission, qui ont finalement un intérêt significatif à ce que la notification n'ait pas lieu pour éviter que l'État, chargé de la mise en œuvre, n'invoque des motifs de refus. En outre, le règlement ne prévoit pas le cas de la notification à l'État dans lequel la personne concernée a son siège ou son domicile. Cela peut s'avérer problématique, en particulier lorsque ni l'autorité d'émission, ni l'autorité chargée de la mise en œuvre n'ont connaissance d'éventuelles immunités prévues par le droit de l'État tiers dans lequel est domiciliée la personne concernée[16].

[16] Voir à ce sujet l'avis critique de l'ONG European Digital Rights (EDRi), e-Evidence compromise blows a hole in fundamental rights safeguards, disponible sous : https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/

2.4.6 Motifs de refus

Le règlement énumère plusieurs motifs de refus qui peuvent être invoqués à l'encontre d'une injonction de production ou de conservation tant par les destinataires d'une injonction que par l'État chargé de la mise en œuvre (à savoir son autorité centrale compétente pour recevoir les notifications).

Le destinataire d'une injonction (fournisseur de services) peut faire valoir que l'injonction enfreint des immunités, des privilèges, la liberté de la presse ou la liberté d'expression conformément au droit de l'État chargé de la mise en œuvre. En présence d'un tel grief, l'autorité d'émission doit décider s'il y a lieu de retirer, d'adapter ou de maintenir l'injonction (art. 10, par. 5 et art. 11, par. 4 du règlement).

Dans le même temps, l'État chargé de la mise en œuvre – à savoir l'autorité centrale chargée de recevoir les notifications – peut refuser une injonction (art. 12, par. 1 du règlement) :

- lorsque les données demandées sont protégées par des immunités ou des privilèges ou par la garantie de la liberté de la presse ou de la liberté d'expression, en vertu de son droit national ;
- dans des cas exceptionnels, lorsqu'il existe des motifs sérieux de croire, sur la base d'éléments précis et objectifs, que l'exécution de l'injonction entraînerait, en tenant compte des circonstances particulières de l'espèce, une violation manifeste d'un droit fondamental pertinent énoncé à l'art. 6 du traité sur l'Union européenne (TUE)[17] et dans la Charte des droits fondamentaux de l'Union européenne (Charte de l'UE) ;
- lorsque l'exécution de l'injonction serait contraire au principe *ne bis in idem*, ou
- lorsqu'il n'existe pas de double incrimination, à savoir que les faits pour lesquels l'injonction a été émise ne constituent pas une infraction au titre du droit de l'État chargé de la mise en œuvre, à moins qu'ils ne concernent une infraction figurant dans les catégories d'infractions énumérées à l'annexe IV, si ces faits sont passibles dans l'État d'émission d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins trois ans.

Selon les ONG, le fait que le motif de refus inhérent aux droits humains soit limité à des situations exceptionnelles de violation des droits fondamentaux pourrait avoir pour effet de désavantager particulièrement les personnes qui résident dans des États, qui connaissent des défis sur le plan de l'État de droit, car ces personnes ne seraient plus en mesure de se protéger en recourant volontairement à un fournisseur de services établi dans un autre État. On pense par exemple aux militants des droits humains[18].

2.4.7 Exécution

Lorsqu'une notification à l'autorité chargée de la mise en œuvre au sens de l'art. 8 du règlement est nécessaire et que cette autorité n'a pas émis d'objections contre la production dans le délai prévu (cf. ch. 2.4.5), le fournisseur de services est tenu de transmettre les données demandées à la fin d'une période de dix jours directement à l'autorité d'émission compétente ou aux autorités de poursuite pénale indiquées dans l'injonction (art. 10, par. 2 du règlement). Lorsque l'autorité chargée de la mise en œuvre confirme avant même l'expiration du délai de dix jours qu'elle n'invoquera aucun motif de refus, le fournisseur de services est tenu d'agir dès que possible après cette confirmation et au plus tard à l'expiration de ce délai de dix jours. Lorsqu'une notification à l'autorité chargée de la mise en œuvre n'est pas nécessaire, le

[17] L'art. 6 TUE dispose notamment que les droits fondamentaux tels qu'ils sont garantis par la CEDH et tels qu'ils résultent des traditions constitutionnelles communes aux États membres font partie du droit de l'Union en tant que principes généraux.

[18] Voir à ce sujet l'avis critique de l'ONG European Digital Rights (EDRi), e-Evidence compromise blows a hole in fundamental rights safeguards, disponible sous : https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/

fournisseur de services est tenu de transmettre les données directement à l'autorité d'émission ou aux autorités de poursuite pénale indiquées dans un délai de dix jours (art. 10, par. 3, du règlement).

En cas d'urgence, le fournisseur de services est tenu de transmettre les données demandées sans retard injustifié, au plus tard dans les huit heures suivant la réception de l'injonction de production (art. 10, par. 4, du règlement). Dans les cas où une notification à l'autorité chargée de la mise en œuvre est nécessaire (à savoir en présence de données relatives au trafic et au contenu), celle-ci peut notifier à l'autorité d'émission et au destinataire, au plus tard dans les 96 heures suivant la réception de la notification, ses objections ou les conditions auxquelles elle entend soumettre l'utilisation des données. Si les données ont déjà été produites, l'autorité d'émission doit les effacer ou restreindre d'une autre manière leur utilisation. Le point problématique est que la production des données a déjà eu lieu alors qu'il s'avère *a posteriori* qu'elle n'était pas autorisée.

Lorsque le fournisseur de services ne peut pas s'acquitter de la production ou de la conservation des données parce que l'injonction est incomplète, contient des erreurs manifestes ou ne contient pas suffisamment d'informations pour être exécutée, ou en raison d'une impossibilité de fait due à des circonstances qui ne lui sont pas imputables, il est tenu d'en informer sans délai l'autorité d'émission (art. 10, par. 6 et 7, et 11, par. 5 et 6, du règlement) ; si l'injonction a été notifiée à l'autorité chargée de la mise en œuvre en vertu de l'art. 8 du règlement, il doit aussi informer cette dernière.

L'injonction de conservation des données prend fin automatiquement après soixante jours, à moins que l'autorité d'émission ne confirme qu'une injonction de production ultérieure a été émise (art. 11 du règlement). Au cours de cette période de soixante jours, l'autorité d'émission peut prolonger la durée de la conservation de trente jours.

2.4.8 Information de l'utilisateur

L'autorité d'émission est tenue d'informer la personne concernée, sans retard injustifié, au sujet de la production de données (art. 13 du règlement). De plus, la section H de l'annexe I du règlement prévoit l'interdiction expresse pour le fournisseur de données d'informer la personne dont les données sont demandées, et dispose qu'il incombe à la seule autorité d'émission d'informer cette personne concernant la production des données. L'autorité d'émission peut, conformément au droit national de l'État d'émission, retarder ou limiter l'information de la personne dont les données sont demandées, ou ne pas informer cette personne, dans la mesure où, et aussi longtemps que, les conditions de l'art. 13, par. 3 de la directive de l'UE sur la protection des données[19] sont remplies. Dans ce cas, l'autorité d'émission indique dans le dossier les raisons du retard, de la limitation de l'information ou de la non-information et ajoute une brève justification dans l'injonction de production.

Le règlement ne règle pas expressément la manière dont la personne concernée doit être informée lorsqu'elle ne se trouve pas sur le territoire de l'autorité d'émission. Sur la base du texte de l'art. 13, qui mentionne uniquement l'autorité d'émission, il y a lieu de présumer que l'information est transmise en tous les cas par l'autorité d'émission, indépendamment du lieu de domicile de la personne concernée (qui peut être situé dans un État tiers). Par exemple, si une autorité allemande demande à un fournisseur de services français des données

[19] Voir l'art. 13, par. 3 : les États membres peuvent adopter des mesures législatives visant à retarder ou limiter la fourniture des informations à la personne concernée [...], ou à ne pas fournir ces informations, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour : a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires ; b) éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes, aux poursuites en la matière ou à l'exécution de sanctions pénales ; c) protéger la sécurité publique ; d) protéger la sécurité nationale ; e) protéger les droits et libertés d'autrui.

concernant une personne qui est domiciliée en France, c'est l'autorité allemande qui doit informer cette personne.

2.4.9 Sanctions et mise en œuvre

2.4.9.1 Sanctions

Les États membres doivent déterminer les sanctions pécuniaires applicables aux fournisseurs de services en cas de violations des art. 10 (exécution d'une injonction de production), 11 (exécution d'une injonction de conservation) et 13, par. 4 (confidentialité, secret et intégrité). Les sanctions pécuniaires prévues doivent être effectives, proportionnées et dissuasives et peuvent aller jusqu'à 2 % du chiffre d'affaires annuel mondial total du fournisseur de services pour l'exercice précédent (art. 15, par. 1 du règlement).

Les fournisseurs de services ne peuvent pas être tenus responsables du préjudice causé à leurs utilisateurs ou à des tiers qui résulte exclusivement du respect de bonne foi d'une injonction de production ou de conservation (art. 15, par. 2, du règlement).

2.4.9.2 Mise en œuvre

Lorsque le fournisseur de services ne respecte pas une injonction de production ou de conservation dans les délais impartis sans indication de motifs et que l'autorité de mise en œuvre n'a invoqué aucun des motifs de refus énumérés à l'art. 12, l'autorité d'émission peut demander à l'autorité chargée de la mise en œuvre de mettre en œuvre l'injonction de production ou de conservation (art. 16, par. 1 du règlement).

L'autorité chargée de la mise en œuvre doit statuer sans délai sur la reconnaissance de la décision de mise en œuvre, au plus tard dans un délai de cinq jours suivant la réception de la décision (art. 16, par. 2 du règlement).

L'autorité chargée de la mise en œuvre enjoint au fournisseur de services d'honorer ses obligations et l'informe dans le même temps :

- de la possibilité de former opposition contre l'exécution de l'injonction concernée en invoquant l'un des motifs de refus mentionnés dans l'injonction (cf. ch. 2.4.6). Si le fournisseur de services fait usage de cette possibilité, l'autorité chargée de la mise en œuvre doit décider sur la base des informations du fournisseur de services d'exécuter ou non l'injonction de production ou de conservation. Pour ce faire, elle peut demander des informations supplémentaires à l'autorité d'émission ;
- des sanctions / amendes applicables en cas de non-respect ;
- du délai pour se conformer à l'injonction ou formuler une objection.

La mise en œuvre d'une injonction de production ou de conservation peut être refusée par l'autorité chargée de la mise en œuvre dans un certain nombre de cas réglés de manière exhaustive dans le règlement, à savoir :

- lorsque l'injonction européenne de production n'a pas été émise ou validée par une autorité d'émission prévue à l'art. 4 ;
- lorsqu'elle n'a pas été émise pour une infraction prévue dans le règlement ;
- lorsque le fournisseur de services n'a pas pu se conformer à une injonction de production ou de conservation pour des motifs qui ne lui sont pas imputables ou parce que l'injonction contient des erreurs graves ;
- lorsque l'injonction de production ne concerne pas des données stockées par le fournisseur de services ou pour son compte au moment de la réception de l'injonction ;
- lorsque le service n'entre pas dans le champ d'application du règlement ;

- lorsque les données demandées sont protégées par des immunités ou des privilèges accordés, en vertu du droit de l'État chargé de la mise en œuvre, ou qu'elles sont couvertes par des règles relatives à la limitation de la responsabilité pénale, liées à la liberté de la presse ou à la liberté d'expression dans d'autres médias, qui empêchent l'exécution ou la mise en œuvre de l'injonction de production ;
- dans des situations exceptionnelles, lorsque sur la base des seules informations contenues dans l'injonction, il est évident qu'il existe des motifs sérieux de croire, sur la base d'éléments de preuve précis et objectifs, que l'exécution de l'injonction européenne de production entraînerait, dans les circonstances particulières de l'espèce, une violation manifeste d'un droit fondamental pertinent énoncé à l'art. 6 TUE et dans la Charte de l'UE.

L'autorité chargée de la mise en œuvre doit informer immédiatement l'autorité d'émission et le fournisseur de services de sa décision. Si l'autorité chargée de la mise en œuvre obtient du destinataire les données demandées dans l'injonction européenne de production, elle doit transmettre ces données sans délai à l'autorité d'émission.

Lorsqu'un fournisseur de services ne respecte pas les obligations, qui lui incombent conformément à une injonction de production ou de conservation dont le caractère exécutoire a été confirmé par l'autorité chargée de la mise en œuvre, cette autorité lui impose une sanction pécuniaire conformément à l'art. 15 du règlement.

2.4.10 Obligations juridiques contradictoires

Lorsqu'un fournisseur de services considère que la production des données demandées est en conflit avec une obligation découlant du droit applicable d'un pays tiers, il est tenu d'informer l'autorité d'émission et l'autorité chargée de la mise en œuvre des motifs pour lesquels il refuse l'exécution de l'injonction de production, dans un délai de dix jours à compter de la réception de celle-ci. Le refus ne peut se fonder sur le fait que le droit applicable de l'État tiers concerné ne contient pas de conditions ou de procédures similaires pour l'émission d'une injonction de production ni sur le seul fait que les données sont stockées dans un État tiers (art. 17, par. 1 s. du règlement).

Lorsque l'autorité d'émission entend maintenir l'injonction malgré le refus motivé, le tribunal compétent de l'État d'émission tranche le conflit. Il doit évaluer dans un premier temps s'il existe un conflit d'obligations, en examinant si le droit de l'État tiers est applicable aux circonstances spécifiques du cas d'espèce et, le cas échéant, si le droit de l'État tiers proscrit la communication des données concernées dans le cas concret. Si le tribunal constate qu'il n'existe pas de conflit au sens indiqué ci-dessus, il maintient l'injonction. Si en revanche, il parvient à la conclusion que le droit de l'État tiers proscrit la production des données concernées, il décide s'il y lieu de maintenir ou de lever l'injonction. Les critères sur lesquels doit se fonder cette évaluation sont énumérés en détail dans le règlement (art. 17, par. 6 du règlement).

Sur ce point, on peut à tout le moins se demander dans quelle mesure le tribunal de l'État d'émission peut effectivement être considéré comme une instance « neutre », lorsqu'il est amené à évaluer les intérêts de sa propre autorité d'émission au regard des intérêts d'un État tiers.

2.5 Voies de droit

Les voies de droit sont réglées à l'art. 18 du règlement, qui prévoit que la personne dont les données sont demandées a droit à des recours effectifs contre l'injonction de production. Si

cette personne est une personne suspecte ou prévenue, elle a droit à des recours effectifs pendant la procédure pénale dans le cadre de laquelle les données sont utilisées.

Le droit à des recours effectifs existe sans préjudice du droit de recours prévu par le RGPD.

Il doit être exercé devant un tribunal de l'État d'émission conformément au droit de cet État. Il comprend la possibilité de contester la légalité de la mesure, y compris sa nécessité et sa proportionnalité, sans préjudice des garanties des droits fondamentaux dans l'État chargé de la mise en œuvre.

Si la personne dont les données sont demandées est informée par l'État d'émission de la production de données, conformément à l'art. 13, par. 1 du règlement, cet État doit l'informer, également en temps utile, sur les possibilités de former un recours prévu par le droit national.

L'État d'émission est tenu de veiller à ce que ces recours puissent être effectivement exercés (art. 18, par. 3 du règlement). La formation de recours est régie par les délais et autres conditions applicables dans le cadre de procédures nationales similaires. À cet égard, il y a lieu de garantir que la personne concernée puisse exercer ces recours de manière effective.

Indépendamment des règles de procédure nationales, l'État d'émission et tout autre État membre auquel des preuves électroniques ont été transmises, en vertu du règlement, doivent garantir que les droits de la défense et l'équité de la procédure sont respectés lors de l'évaluation des preuves obtenues au moyen de l'injonction de production.

2.6 Système informatique décentralisé

Le paquet e-evidence prévoit la création d'un système informatique décentralisé destiné à garantir la fiabilité de la communication électronique et de l'échange de données entre les autorités compétentes et les fournisseurs de services ou uniquement entre les autorités compétentes.

Les établissements ou les représentants légaux désignés par les fournisseurs de services doivent avoir accès au système informatique décentralisé par l'intermédiaire de leurs systèmes informatiques nationaux respectifs afin de recevoir les injonctions de production et de conservation, de transmettre les données demandées et de communiquer avec les autorités compétentes.

Les coûts inhérents à l'installation, à l'exploitation et à la maintenance des points d'accès décentralisés du système informatique sont à la charge des États membres concernés. De plus, chaque État membre prend en charge les coûts relatifs à l'établissement et à l'adaptation de ses systèmes informatiques nationaux, afin de les rendre compatibles entre eux.

2.7 Délai de mise en œuvre

Le délai de mise en œuvre du paquet e-evidence est de 36 mois et a commencé à courir le 28 juillet 2023 au moment de la publication au Journal officiel de l'Union européenne[20].

3 Droit comparé

Le paquet e-evidence n'aura pas seulement des conséquences sur la Suisse, mais également sur d'autres États dont les fournisseurs de services exercent leur activité dans l'UE. C'est pourquoi la Suisse a pris contact avec plusieurs États afin d'échanger concernant leur position

[20] JO L 191 du 28 juillet 2023, p. 118

relative aux nouvelles règles de l'UE. Toutefois, la plupart de ces États n'ont pas encore procédé à une analyse détaillée du nouveau paquet législatif.

Le **Royaume-Uni** a conclu un *executive agreement* avec les États-Unis sur la base du CLOUD Act. En raison de son départ de l'UE, le Royaume-Uni ne sera pas tenu par la réglementation e-evidence. Il n'a pas encore pris position concernant le paquet e-evidence. Au vu de son adhésion au système du CLOUD Act américain, il semble peu probable que le pays s'intéresse de manière approfondie à la réglementation européenne.

L'**Islande** et la **Norvège**, deux États qui sont dans une situation similaire à celle de la Suisse, en ce sens qu'ils ne sont pas non plus membres de l'UE mais ont développé une forte coopération avec cette dernière en tant qu'États Schengen dans les domaines concernés, ne semblent pas non plus avoir entamé d'analyse au sujet du paquet e-evidence et de la coopération pénale internationale dans le domaine des preuves électroniques. Contrairement à la Norvège et à la Suisse, l'Islande a signé le Deuxième Protocole additionnel à la convention sur la cybercriminalité.

La Suisse a également eu des échanges avec le **Danemark**. Bien qu'il soit membre de l'UE, il dispose d'une option de retrait en ce qui concerne l'espace de liberté, de sécurité et de justice, ce qui signifie qu'il ne met pas en œuvre les règlements fondés sur ce domaine de compétences de l'UE. Comme mentionné plus haut, alors que le règlement est basé sur l'espace de liberté, de sécurité et de justice, ce n'est pas le cas de la directive e-evidence, raison pour laquelle le Danemark doit mettre en œuvre la directive mais pas le règlement. Cependant, la directive prévoit en substance que les États qui ne participent pas au règlement doivent prendre les mesures nécessaires pour que les fournisseurs de services établis sur leur territoire nomment un représentant légal dans l'UE. Le Danemark est actuellement en train d'analyser la manière de mettre en œuvre la directive sans le règlement.

La situation de l'**Irlande** est différente puisqu'elle dispose d'une option de retrait flexible, qui lui permet de décider de manière autonome à quels projets législatifs elle souhaite participer dans le domaine de l'espace de liberté, de sécurité et de justice. En raison du grand nombre de fournisseurs de services établis sur son territoire, l'Irlande a un intérêt particulier à participer au paquet e-evidence afin d'éviter que ces fournisseurs de services ne soient contraints de désigner un représentant dans un autre État membre de l'UE. Cependant, le règlement renvoie à certains instruments auxquels l'Irlande n'a pas adhéré.

L'Irlande a indiqué peu après le Brexit, alors que les négociations du paquet e-evidence étaient en cours, qu'elle entendait participer à cette initiative. Aussi est-elle en train de modifier son droit national afin que les injonctions européennes de production et de conservation prises sur la base du paquet e-evidence puissent être adressées directement aux fournisseurs de services établis en Irlande. Elle espère pouvoir mettre en œuvre le règlement même si elle n'a pas repris tous les instruments sur lesquels se fondent ses dispositions (par exemple, la décision d'enquête européenne). En modifiant son droit national, elle vise une mise en œuvre de la directive dès son entrée en vigueur.

Enfin, les **États-Unis** et l'UE négocient, depuis plusieurs années, un accord qui règlerait l'accès aux preuves électroniques entre les deux entités. Si les médias et le *Departement of justice* américain parlent principalement d'un *executive agreement*, les informations en possession de la Suisse semblent plutôt indiquer que les deux entités négocient un accord international indépendant qui permettrait de créer un pont entre le système américain et le système européen. Après une période de gel des négociations en 2020 en raison d'une part de la pandémie et d'autre part des délibérations relatives au paquet e-evidence dans l'UE, les

discussions ont maintenant repris. Il semble que l'instrument en cours de négociation ait pour but d'éviter que les fournisseurs de service soient soumis à des obligations contradictoires puisqu'ils seraient assujettis dans les faits tant au CLOUD Act qu'au projet e-evidence.

4 Conséquences pour la Suisse

S'il est vrai que le paquet e-evidence aura principalement des conséquences pour les États membres de l'UE, ou en tout cas pour ceux qui y participent, il devrait avoir également des répercussions sur la Suisse, non seulement au vu de sa proximité territoriale avec l'UE, mais également en raison des liens étroits qu'elle entretient avec les États de l'UE. Ces répercussions concerneront principalement les fournisseurs de services établis en Suisse, mais pas uniquement.

4.1 Conséquences pour les fournisseurs de services

Les fournisseurs de services établis en Suisse qui proposent ou souhaitent proposer sur le marché européen des services couverts par le paquet e-evidence (cf. ch. 2.3.1), seront soumis à la réglementation de l'UE.

Il en résulte d'une part qu'ils devront désigner un représentant légal dans un État membre de l'UE, dans la mesure où ils n'y transfèrent pas leur établissement, et d'autre part, que les autorités européennes de poursuite pénale pourront adresser directement leurs injonctions de production et de conservation à ce représentant. Le fournisseur de services devra se conformer à ces injonctions, ce qui signifie qu'il devra produire ou conserver les données demandées par une autorité de poursuite pénale de l'UE en vue d'une procédure pénale en dehors de la Suisse. Cela entraîne le risque que des données stockées en Suisse soient transmises à l'étranger sans recours à l'entraide pénale internationale et aux garanties de procédure qu'elle offre.

De plus, il incombera aux fournisseurs de services établis en Suisse d'invoquer d'éventuels conflits de lois ou violations du droit suisse. Lorsqu'un fournisseur de services invoquera un tel conflit de lois, le tribunal de l'État d'émission devra statuer à ce sujet. Partant, il reviendra aux fournisseurs de services, et donc à des entités privées, de veiller au respect du droit suisse et d'éviter d'éventuels conflits de lois entre les obligations du fournisseur de services conformément au droit suisse et celles issues du paquet e-evidence.

4.2 Autres conséquences

La Suisse et l'UE ont développé depuis de nombreuses années des relations privilégiées fondées sur les accords bilatéraux. La coopération internationale en matière pénale entre la Suisse et l'UE et ses États membres se fonde sur les instruments du Conseil de l'Europe et est complétée par l'association de la Suisse à l'accord de Schengen[21] et à l'accord sur la lutte contre la fraude[22]. Le paquet e-evidence ne fait pas partie de la coopération Schengen ni d'un autre accord bilatéral entre la Suisse et l'UE. C'est pourquoi, outre les effets mentionnés ci-dessus pour les fournisseurs de services établis en Suisse, le paquet e-evidence n'aura pas de conséquences directes pour la Suisse lors de son entrée en vigueur.

Afin de pouvoir continuer à lutter efficacement contre la criminalité, la Suisse devra adapter sa législation en matière de preuves électroniques. La Suisse ne peut faire cavalier seul, car une législation purement nationale ne saurait garantir un accès transfrontalier effectif aux données

[21] Accord entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen, RS 0.362.31

[22] Accord de coopération entre la Confédération suisse, d'une part, et la Communauté européenne et ses États membres, d'autre part, pour lutter contre la fraude et toute autre activité illégale portant atteinte à leurs intérêts financiers, RS 0.351.926.8

en tant que moyens de preuve dans le cadre de procédures pénales. Dans le cadre d'une action législative isolée, la Suisse devrait au contraire être en mesure d'obtenir la présence et la coopération de tous les fournisseurs de services concernés en Suisse. Au vu des rapports de force géopolitique, cela ne semble guère réaliste. C'est pourquoi la dimension transfrontalière de l'accès aux données restera très importante pour la Suisse dans la pratique. L'UE étant un partenaire important de la Suisse dans de nombreux domaines,, il est indispensable que la Suisse intègre le paquet e-evidence, ses opportunités et ses risques, dans ses réflexions sur la réorganisation de la collecte des preuves électroniques.[23].

Par ailleurs, le paquet e-evidence prévoit la mise en place d'un registre des fournisseurs de services. Si un tel registre venait à être disponible, par exemple par le biais d'Eurojust, il serait utile aux autorités suisses pour savoir dans quel État les fournisseurs de services ont un établissement. Elles pourraient adresser leurs demandes d'entraide directement au bon État.

5 Différences entre le paquet e-evidence et le US Cloud Act

Le CLOUD Act et le paquet e-evidence de l'UE poursuivent tous deux l'objectif de faciliter l'accès aux preuves électroniques et de lutter plus efficacement contre la criminalité transnationale. Les prochains paragraphes mettent en évidence les différences et similarités entre les deux instruments.

5.1 Territorialité et accès transnational

La première différence concerne la question de la territorialité. Le paquet e-evidence de l'UE vise tous les fournisseurs de services qui proposent leurs services dans l'UE, avec pour conséquence que les fournisseurs de services qui sont établis en dehors de l'UE devront y nommer un représentant légal. Le CLOUD Act se concentre quant à lui sur le lien étroit que doit avoir un fournisseur de services avec les États-Unis. Il s'applique aux fournisseurs de services établis sur le territoire américain ou qui y ont une filiale ou une succursale. Dans certains cas, il s'applique même à ceux qui font de la publicité pour leurs services sur le marché américain. Le CLOUD Act ne se fonde pas sur le critère de la présence aux États-Unis et n'exige pas non plus que les fournisseurs de services qui y sont soumis aient une telle présence sur le territoire américain. Les fournisseurs de services sont tenus de produire les données qui se trouvent sur leurs serveurs, indépendamment du fait que les données soient stockées aux États-Unis ou à l'étranger. Des injonctions de production en vertu du CLOUD Act peuvent notamment être adressées à un établissement suisse d'un fournisseur de services aux États-Unis. Si de tels accès « extraterritoriaux » aux données ne posent pas de problème dans le système juridique américain, ils peuvent cependant engendrer des conflits avec les systèmes juridiques des États où se trouvent les données. En revanche, le système de l'UE « domestique » les données. En raison de l'obligation de présence des fournisseurs de services, aucune injonction n'est jamais envoyée dans des territoires situés en dehors de l'UE, mais elle est toujours adressée au siège ou au représentant légal désigné dans l'UE. Toutefois, ce dernier doit également avoir accès à toutes les données de l'entreprise, indépendamment de l'endroit où elles sont stockées. Les fournisseurs de services qui sont concernés par le règlement de l'UE doivent transmettre toutes les données de leur entreprise, indépendamment du lieu où celles-ci sont stockées.

Les deux systèmes prévoient un accès transnational aux données, et simplifient l'accès transfrontalier aux données. Alors que le système de l'UE « oblige » les fournisseurs de services à être présents sur le territoire de l'UE et exige l'accès à toutes les données de l'entreprise depuis la centrale de l'UE, le système américain se base sur les liens des

[23] Voir les réflexions figurant au ch. 6.

fournisseurs de services avec les États-Unis. Un fournisseur de services qui a ce lien avec le système juridique américain, tel qu'il est compris par les États-Unis, est tenu de fournir toutes ses données, quel que soit l'endroit où elles se trouvent.

En outre, le CLOUD Act prévoit la possibilité de conclure des *executive agreements* qui permettent aux autorités américaines d'envoyer des demandes aux fournisseurs de services qui ne sont pas établis sur le territoire américain mais se trouvent dans des États avec lesquels un *executive agreement* a été conclu et vice et versa.

5.2 Protection des données à caractère personnel et des droits humains

Tant le CLOUD Act que le paquet e-evidence contiennent des dispositions relatives à la protection des données. Les dispositions du paquet e-evidence doivent respecter les standards de protection des données de l'UE, en particulier le RGPD. La Suisse n'étant pas membre de l'UE, le RGPD ne s'y applique pas directement puisqu'il ne s'agit pas d'un développement de l'acquis de Schengen. Toutefois, la Suisse a révisé sa législation en matière de protection des données afin de tenir compte de l'évolution intervenue dans ce domaine sur le plan international et européen. La nouvelle mouture de la loi sur la protection des données (LPD, RS 235.1) est entrée en vigueur le 1er septembre 2023. Les dispositions du RGPD s'appliquent à des entreprises en Suisse qui relèvent du champ d'application du règlement (art. 3 RGPD). C'est le cas lorsque le fournisseur de services est établi dans l'UE ou, à défaut d'établissement, lorsque le traitement des données s'inscrit dans le cadre de l'offre de biens ou de services dans l'UE à des personnes concernées ou du suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

La Suisse dispose d'une décision d'équivalence de l'UE qui la reconnaît comme un État tiers disposant d'un niveau adéquat de protection des données, ce qui permet un échange de données sans obstacle. Elle peut donc considérer que l'application du paquet e-evidence remplira les standards européens en la matière et ne compromettra pas cette équivalence, puisque les entreprises visées seront soumises tant aux règles européennes qu'aux règles suisses.

En revanche, les standards de protection des données prévus par le CLOUD Act diffèrent des standards suisses. Le rapport CLOUD Act parvient à la conclusion que le traitement des données effectué dans le cadre d'une procédure basée sur le CLOUD Act peut être qualifié de problématique à la lumière de plusieurs éléments du RGPD[24].

Sur le plan des droits humains, le droit suisse a davantage de points communs avec les dispositions en matière d'e-evidence qu'avec celles du CLOUD Act. Les États membres de l'UE sont tous membres du Conseil de l'Europe et sont soumis de ce fait à la Convention européenne des droits de l'homme (CEDH). Le paquet e-evidence sera appliqué en concordance avec cet instrument auquel la Suisse est également partie. Cela concerne en particulier la garantie de l'accès au juge consacrée à l'art. 6 CEDH et à l'art. 29*a* Cst. Les dispositions du paquet e-evidence garantissent également le droit à des recours effectifs à la personne concernée par le transfert des données. Le CLOUD Act ne prévoit pas la possibilité pour la personne concernée d'accéder à un juge.

5.3 Aspects procéduraux

Tant le CLOUD Act que le paquet e-evidence prévoient que les injonctions sont transmises directement par les autorités d'un État à un fournisseur de services dans un autre État. Les

[24] OFJ, rapport CLOUD Act, pp. 23 ss.

autorités de l'État dans lequel se trouve le fournisseur de services ne participent en principe pas à la collecte des données. On pourrait parler de « privatisation de l'entraide pénale internationale ». Dans le paquet e-evidence, cet effet est quelque peu nuancé par l'obligation de notification. Si la demande porte sur la production de données relatives au trafic ou au contenu, l'autorité d'émission est tenue d'informer de l'injonction tant le fournisseur de services que l'autorité compétente dans l'État dans lequel le fournisseur de services est établi ou a désigné un représentant légal (cf. ch. 2.4.5).

Ce mécanisme n'est pas prévu par le CLOUD Act ni par l'*executive agreement* conclu entre les USA et le Royaume-Uni. L'État sur le territoire duquel se trouve le fournisseur de services n'a aucune connaissance des demandes reçues par les fournisseurs qui se trouvent sur son territoire, et ce malgré l'*executive agreement*.

Un autre aspect important qu'il sied de mentionner est celui de l'utilisation de la contrainte ou de l'exécution des injonctions. Le CLOUD Act prévoit que les autorités de poursuite pénale ne peuvent utiliser aucune mesure de contrainte sur le territoire d'un autre État. Si un fournisseur de services d'un État ayant conclu un *executive agreement* avec les États-Unis refuse de transmettre les données demandées, les autorités américaines doivent passer par la voie de l'entraide pénale internationale pour obtenir ces données. Quant au paquet e-evidence, il prévoit que l'injonction est dans ce cas mise en œuvre au moyen des mécanismes prévus par le règlement sans passer par l'entraide judiciaire. Une autorité d'émission d'un État membre de l'UE peut, moyennant le respect des procédures prévues par le règlement (cf. ch. 1.4.9), prononcer une sanction financière à l'encontre d'un fournisseur de services qui se trouve sur le territoire d'un autre État membre de l'UE.

Le paquet e-evidence institue un registre central des établissements et représentants légaux des fournisseurs qui offrent dans l'UE des services entrant dans le champ d'application du règlement. Grâce à ce registre, les autorités de poursuite pénale sont en mesure d'adresser rapidement leurs demandes aux entités compétentes. Le CLOUD Act ne met pas en place ce type de registre.

Ni le CLOUD Act, ni le paquet e-evidence n'ont d'effet en matière de chiffrement des données. Aucun de ces instruments ne prévoit l'obligation pour les fournisseurs de données de décrypter les données en leur possession avant de les envoyer, ce qui pourrait engendrer quelques difficultés pratiques pour les autorités de poursuite pénale.

5.4 Ouverture à d'autres États

Le CLOUD Act prévoit la possibilité, pour les États qui le souhaitent et qui remplissent certains critères sur le plan de l'État de droit du point de vue des États-Unis, de conclure des *executive agreements* avec ces derniers, sur la base desquels les autorités d'autres États pourront faire parvenir des injonctions directement aux fournisseurs de services américains et vice et versa. Au vu de la mondialisation croissante, un tel système ouvert permettra d'accélérer la coopération internationale et de mieux lutter contre la criminalité de manière générale.

Le paquet e-evidence ne contient pas de possibilité d'ouverture à d'autres États, bien au contraire : étant donné qu'il repose sur plusieurs actes de l'UE, notamment sur des mécanismes visant à simplifier l'entraide comme la décision d'enquête européenne, il serait difficile pour un État tiers d'adhérer à ce système par la voie bilatérale.

5.5 Conflits de lois

Les deux systèmes prévoient des règles relatives à d'éventuels conflits de lois. Les règles prévues par le CLOUD Act sont toutefois très limitées : seul le fournisseur de services – et non l'État dans lequel il a son siège – est autorisé à invoquer un tel conflit de lois, et uniquement à la condition qu'un *executive agreement* ait été conclu. C'est l'État qui demande les données qui doit ensuite décider s'il existe ou non un conflit de lois dans le cas d'espèce.

Dans le cadre du système e-evidence, il revient également principalement au fournisseur de services d'invoquer un conflit de lois avec un État tiers ou l'État dans lequel il a installé son établissement ou a désigné un représentant légal[25]. Le fournisseur doit cependant également informer de son refus l'autorité compétente de l'État dans lequel il a installé son établissement ou désigné un représentant légal. Comme sous l'empire du CLOUD Act, c'est l'État qui demande les informations qui décide si l'on est ou non en présence d'un conflit de lois. Lorsque le fournisseur de services invoque l'un des motifs de refus limités conformément au droit de l'État dans lequel il se trouve, c'est l'autorité d'émission qui décide (cf. ch. 2.4.6) ; en cas d'invocation d'un conflit avec le droit d'un État tiers, la décision incombe au tribunal compétent de l'État d'émission (cf. ch. 2.4.10).

Contrairement au CLOUD Act américain, l'État d'émission doit dans certains cas adresser une notification concernant l'injonction à l'État dans lequel le fournisseur de services a installé son établissement ou désigné son représentant légal. Le fournisseur a ensuite la possibilité de refuser l'injonction en présence de l'un des motifs de refus énumérés de manière exhaustive dans le règlement (cf. ch. 2.4.6)[26].

6 Conclusion

Les règles e-evidence de l'UE représentent une avancée significative dans le domaine de l'accès transfrontalier aux données en tant que moyens de preuves dans le cadre de procédures pénales sur le continent européen. En établissant des règles claires, relatives tant à la présence des fournisseurs de services dans l'UE qu'aux injonctions européennes de production et de conservation, l'UE renforce la coopération internationale en matière pénale en tenant compte – au moins jusqu'à un certain point – des droits fondamentaux des personnes visées par de telles procédures et de la protection de leurs données. Ces nouvelles règles seront amenées à jouer un rôle crucial dans la lutte contre la criminalité transfrontalière.

[25] Étant précisé, en relation avec le droit de l'État dans lequel le fournisseur de services a installé son établissement ou désigné un représentant légal, que les motifs de refus sont limités aux immunités, privilèges et garanties de la liberté de la presse et d'expression prévus par le droit de cet État.

[26] Les motifs de refus ne couvrent pas l'intégralité du droit de l'État chargé de la mise en œuvre, mais sont limités aux immunités, privilèges, garanties de la liberté de la presse et de la liberté d'expression, violations manifestes d'un droit fondamental applicable conformément à la Charte de l'UE ou de l'art. 6 TUE, violation du principe ne bis in idem et absence de double incrimination.

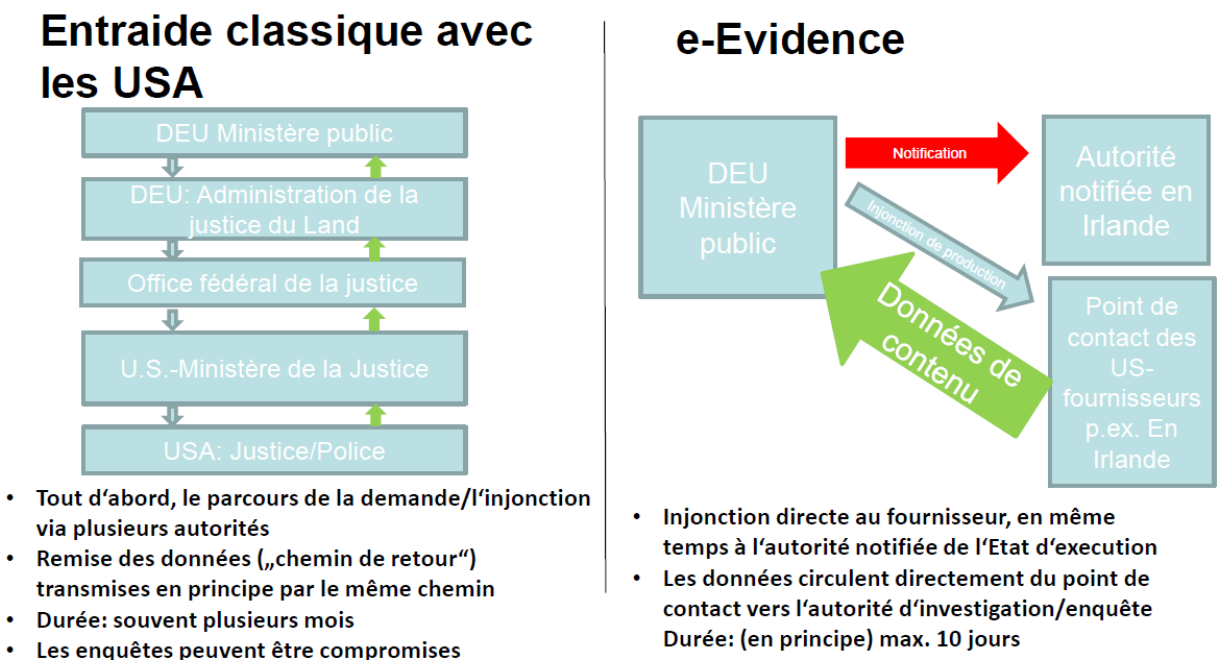

Illustration : accès aux données par un procureur allemand auprès d'un fournisseur de services américain conformément à la réglementation e-evidence et à la procédure d'entraide judiciaire classique (source : ministère allemand de la justice)

Compte tenu de l'évolution des régimes de ses principaux partenaires, la Suisse doit également se pencher sur le thème de l'e-evidence. Actuellement, le droit suisse se fonde uniquement sur l'entraide internationale en matière pénale, qui est relativement lente et n'est pas adaptée aux preuves électroniques. Il ne paraît pas judicieux de faire cavalier seul. Les preuves électroniques remettent en cause le concept de territorialité et sont stockées dans différents États par des entreprises qui ne sont pas toutes soumises au droit suisse. Dans ce contexte, une solution suisse unilatérale semble difficilement envisageable. La Suisse doit être en mesure de coopérer avec d'autres États. À ce stade, plusieurs options sont envisageables.

- La première consiste à ne rien faire. Comme indiqué, il s'agit d'un domaine qui évolue rapidement et qui a de plus en plus souvent des incidences sur les procédures pénales. Ne rien faire aurait pour effet de créer une lacune dont les criminels pourraient se servir. En outre, un conflit de lois serait susceptible de survenir (cf. en particulier l'art. 271 CP)[27] lors de l'entrée en vigueur de la réglementation de l'UE en matière d'e-evidence.

- Le deuxième scénario serait de modifier le droit suisse afin de développer une solution autonome. En y regardant de plus près, ce scénario se décompose en deux options :

  - d'une part, la Suisse pourrait simplement essayer d'éviter les conflits de lois qui découleraient de la réglementation e-evidence. Elle pourrait adapter son droit national de sorte que l'accès étranger aux données soit toléré. Cela serait relativement simple à réaliser sur le plan technique, mais elle accorderait un droit aux autorités étrangères sans recevoir de contrepartie ;
  - d'autre part, la Suisse pourrait essayer de développer une solution autonome qui permettrait d'étendre l'accès des autorités suisses aux données qui ont un lien avec la Suisse. Cela aurait pour avantage qu'elle pourrait développer un droit qui serait conforme à ses propres principes juridiques et qui serait adapté à ses besoins. Cependant, des fournisseurs de services issus du monde entier offrent leurs services en Suisse. En tant que petit pays, il serait difficile pour

[27] Si un fournisseur de services domicilié en Suisse installait un point de contact dans un État de l'UE conformément à la réglementation e-evidence, y recevait des injonctions européennes de production et, sur cette base, produisait des données qui se trouvent en Suisse, il procéderait selon la conception suisse à des actes qui relèvent des pouvoirs publics. Il y aurait là un conflit avec l'art. 271 CP – et le fournisseur de services devrait à chaque fois requérir l'approbation du DFJP, ce qui est difficilement réalisable.

cette dernière d'amener tous ces fournisseurs de services à désigner un représentant légal sur son territoire ou d'y installer un établissement.

- Le troisième scénario pourrait consister en un rattachement à l'un ou l'autre des systèmes décrits ou aux deux. Le paquet e-evidence ne prévoit pas expressément une telle possibilité, contrairement au CLOUD Act. Cependant, l'UE et les États-Unis sont en train de négocier un accord visant à faciliter la coopération internationale dans le domaine des preuves électroniques. La Suisse pourrait tenter de modifier son droit national de manière autonome en tenant compte des deux systèmes et des solutions mises en place pour résoudre les conflits. Cette révision pourrait prévoir la possibilité de créer des ponts vers d'autres systèmes juridiques au moyen d'accords internationaux.
  Compte tenu des liens étroits existant entre la Suisse et l'UE dans les domaines de la coopération judiciaire et de la protection des données (en particulier dans le cadre de la coopération Schengen), eu égard également à la libre circulation des personnes (sur laquelle est fondée la directive e-evidence) et à l'accès au marché intérieur, également dans le domaine du numérique, il semble judicieux d'orienter les efforts non seulement sur les États-Unis, mais également sur l'UE et les États voisins de la Suisse. La question se pose même de savoir si la Suisse pourrait éventuellement élaborer une solution qui se fonde sur la législation e-evidence de l'UE.

Quoiqu'il en soit, la Suisse doit agir, et rapidement. La nouvelle législation e-evidence entrera en vigueur 36 mois après le 28 juillet 2023, à savoir le 28 juillet 2026. Si aucune solution ne devait être trouvée, il existe à partir de cette date le risque de conflit de lois avec le nouveau système de l'UE. Dans ce cadre, il y a lieu de garder à l'esprit que la Suisse ne doit pas mettre en danger ses accomplissements sur le plan de l'État de droit. Elle devrait toutefois viser en principe une solution qui permette à ses autorités de poursuite pénale de coopérer avec d'autres États, ou tout au moins avec des fournisseurs de services qui se trouvent sur le territoire d'autres États.