Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller

Utilisation des services de cloud par les avocates et avocats

Avant-propos

Dans le cadre de la numérisation, les cabinets d'avocats recourent de plus en plus souvent à des fournisseurs de services de nuage informatique (cloud) pour le traitement, l'enregistrement et l'archivage de documents et d'autres données. On trouve même déjà, sur le marché, des services de cloud spécialement adaptés aux besoins des avocats. L'utilisation des services de cloud par les avocats soulève néanmoins un certain nombre de questions de droit pénal et de protection des données, qui font parfois l'objet de controverses en doctrine.

Sur cette toile de fond, la Fédération Suisse des Avocats (FSA) a mandaté en été 2018 le Center for Information Technology, Society, and Law (ITSL) de l'université de Zurich avec un examen approfondi des conditions cadres juridiques de l'utilisation des services de cloud, sous l'angle du droit pénal et du droit de la protection des données. L'ITSL a présenté son avis de droit à l'automne 2018. La publication d'une version complétée et actualisée de cet avis de droit dans la collection de l'ITSL fait écho au souhait de la FSA de porter les résultats de l'avis de droit à la connaissance d'un plus large public.

Les auteurs souhaitent exprimer leurs remerciements à la FSA pour l'agréable collaboration. Les auteurs remercient également Damian George, MLaw, avocat, Rebecca Sigg, MLaw, avocate, Bruno Rodrigues, MSc., Sina Rafati, MSc., et Eder Scheid, MSc., pour leurs travaux de recherche et préliminaires relatifs à différentes parties de l'avis de droit. Leurs remerciements vont aussi à Peter-Conradin Schreiber, étudiant en droit, et Aurelia Tamò-Larrieux, Dr. iur., pour la relecture du manuscrit, ainsi qu'à Geneviève Kaspers-Grandchamp pour la traduction française.

Zurich, en février 2019

CHRISTIAN SCHWARZENEGGER
FLORENT THOUVENIN
BURKHARD STILLER

Table des matières

I. Situation initiale et question

L'utilisation de services informatiques est entrée dans les mœurs de la profession d'avocat depuis de nombreuses années. Outre les logiciels de traitement de texte, les solutions logicielles pour la gestion des mandats, la saisie des prestations et la facturation ainsi que les bases de données en ligne font également partie de l'équipement de base des avocates et avocats.

À ce jour, les solutions locales sous forme d'ordinateurs autonomes («*stand alone*») ou de réseaux locaux sont les plus répandues. Les données que les avocates et avocats reçoivent de leurs clients et celles générées dans l'exercice de leur activité professionnelle – p. ex. celles contenues dans les contrats, les mémoires et la correspondance – sont ainsi traitées et enregistrées soit sur le disque dur de l'ordinateur autonome, soit sur le serveur central du cabinet d'avocats. En règle générale, la mise en place et la maintenance de l'équipement informatique requis ainsi que l'installation et l'actualisation des logiciels ne sont pas assurées par les avocates et avocats eux-mêmes, mais par un informaticien interne ou un prestataire de services informatiques externe. Dans le cadre de leur activité, les collaborateurs en informatique et ceux du prestataire de services informatiques ont inévitablement accès aux données protégées par le secret professionnel de l'avocat.

Depuis peu, les études d'avocats font de plus en plus souvent appel à des fournisseurs de services informatiques en nuage («*cloud providers*») en lieu et place de rechercher des solutions locales.

Dans ce contexte, la Fédération Suisse des Avocats (FSA) a commandé le présent avis de droit destiné à examiner la question de savoir si et, le cas échéant, à quelles conditions les avocates et avocats qui exercent en Suisse font usage de services informatiques en nuage («services de cloud») dans le cadre de leur activité professionnelle, pour traiter, enregistrer et archiver des documents et autres données, respective-

ment s'ils sont en droit de faire appel à des tiers mettant à leur disposition des capacités de mémoire et de calcul.

Deux questions se posent de prime abord: d'une part, il s'agit d'examiner la question de savoir si l'utilisation de services de cloud constitue une violation du secret professionnel des avocates et avocats (III), et d'autre part si, et, le cas échéant, à quelles conditions préalables l'utilisation de services de cloud par les avocates et avocats est compatible avec les exigences du droit de la protection des données (IV). Il convient cependant de clarifier au préalable les fondements techniques (II).

II. Fondements techniques

1. Cloud computing en général

La notion de «cloud» décrit une série de services en ligne accessibles via réseau, depuis presque tous les emplacements et ce, d'une manière telle que le bénéficiaire des prestations ne connaît pas le lieu physique à partir duquel ces prestations sont fournies. L'un des services proposés peut être la «sauvegarde» dans un nuage informatique («cloud») qui – contrairement à ce qui a lieu en cas d'utilisation d'un ordinateur autonome – constitue un système de stockage décentralisé et dispersé au sein duquel toutes les données peuvent être enregistrées sous forme électronique, sans format dédié. En outre, le partage des données se trouve facilité du fait de solutions indépendantes de la technologie utilisée (notamment de l'équipement informatique et des logiciels / du système d'exploitation). La virtualisation sur base de cloud peut permettre aux entreprises de réduire le nombre d'appareils (ordinateurs ou systèmes individuels) et de licences de logiciels requis pour assurer leur exploitation. Les nuages informatiques permettent ainsi couramment d'augmenter l'efficacité et de réduire les coûts de l'exécution ou du soutien à l'exécution des tâches et processus opérationnels récurrents.

Presque toutes les ressources de la technologie de l'information (données, équipement informatique et logiciels) peuvent être délocalisées dans un cloud: un programme, une application, un service, un système d'exploitation destiné à des fins déterminées, voire toute une infrastructure. Si un cabinet d'avocats souhaite mettre en place p. ex. une infrastructure informatique pour le traitement des documents et données de ses clients, il lui est possible d'aménager un nuage informatique regroupant les logiciels, les services et les ressources réseau. Le cabinet d'avocats et, en cas de besoin, des tiers autorisés (dans la mesure où des contrôles d'accès adéquats sont installés) peuvent ainsi accéder aux documents et données, via l'infrastructure cloud.

Dans l'illustration 1, les cabinets d'avocats 1 et 2 exploitent l'infrastructure locale pour leurs collaborateurs. La «mise en nuage» présentée permet d'enregistrer les données auprès d'un fournisseur de cloud – une instance spécifique du prestataire de services informatiques – spécialisé dans la fourniture d'un accès (en écriture et en lecture) à la mémoire de données qui soit sûr, fiable et efficient. Les données typiquement organisées en documents sont cryptées sur le site du cabinet d'avocats (symbole de la clé figurant à côté du symbole du document), et les clés cryptographiques ne sont connues que du cabinet d'avocats, voire d'un seul utilisateur au sein de ce dernier. Les données sont ensuite transférées de manière cryptée via le réseau – ici l'Internet, public. Cet exemple montre clairement que les deux cabinets d'avocats travaillent avec leurs propres clés cryptographiques, qui ne sont connues que par le cabinet respectif, mais qu'ils utilisent le même fournisseur de services de cloud. Ainsi, les données sont enregistrées au sein de l'infrastructure du fournisseur de services de cloud, de telle manière que celui-ci – ou un tiers – ne dispose d'aucune possibilité réaliste de décrypter le contenu de ces données.

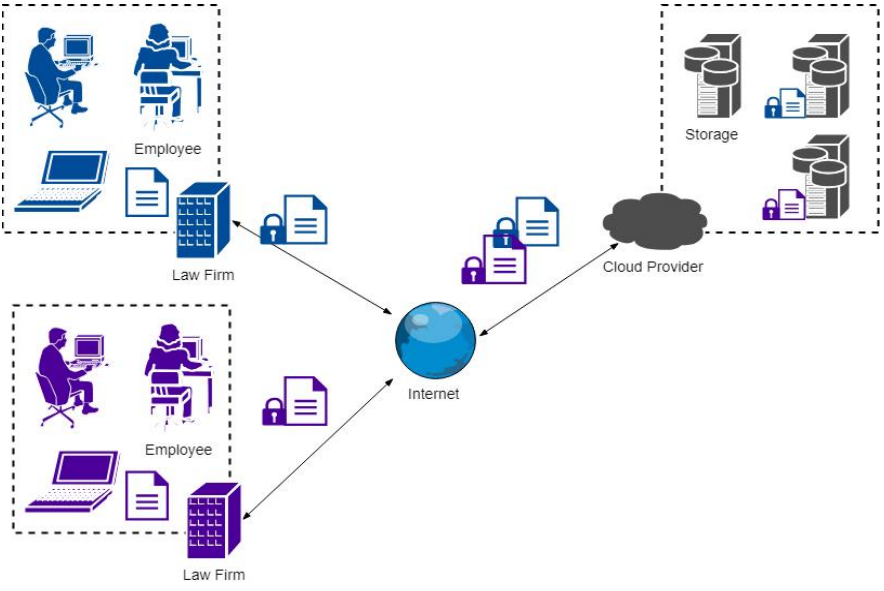

Illustration 1: fonctionnement général du cloud computing

Même si les données des cabinets d'avocats 1 et 2 sont enregistrées au sein d'une seule et même infrastructure du fournisseur de services de cloud, aucun des deux cabinets d'avocats ne peut avoir accès aux données de l'autre parce que, d'une part, il ne connaît pas le lieu de stockage des données dans le nuage informatique du fournisseur de services de cloud et que, d'autre part, il ne dispose pas de la clé cryptographique des données correspondantes. Si l'infrastructure du fournisseur de services de cloud venait à être compromise, les données divulguées n'auraient aucune pertinence sans la clé juste. Comme pour toutes les clés cryptographiques et preuves d'autorisation utilisées dans le monde digital, la probabilité théorique que la clé puisse être calculée par des tiers existe, bien qu'elle soit quasiment nulle. Ainsi, le risque en matière de sécurité est minimal lorsque de solides mesures de sécurité sont mises en place. L'évaluation simple des risques est comparable à celle pour les trésors ou les coffres-forts analogiques, qui peuvent être ouverts au moyen d'une combinaison de chiffres devinée ou volée.

2. Modèles de services de cloud

Le modèle de services de cloud détermine la manière dont l'ensemble configurable de ressources de cloud computing est utilisé et mis à la disposition de l'utilisateur. Le National Institute of Standards and Technology (NIST), la Cloud Security Alliance (CSA) et l'European Union Agency for Network and Information Security (ENISA) ont réparti ces services en trois catégories principales, qui sont les suivantes: Infrastructure-as-a-Service (IaaaS), Platform-as-a-Service (PaaS) et Software-as-a-Service (SaaS). Voir à ce propose l'illustration 2.

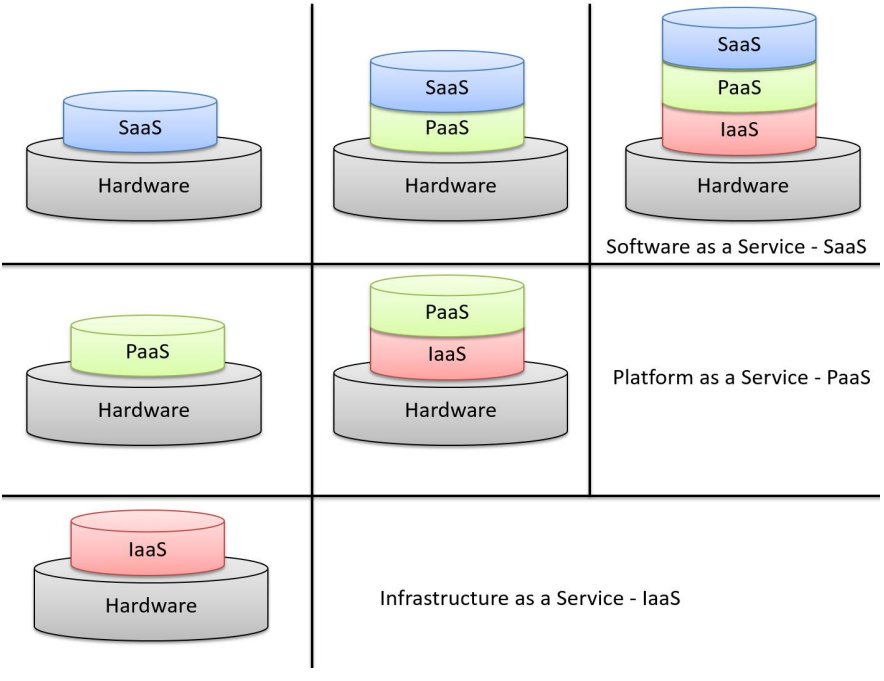

Illustration 2: modèles de services de cloud computing

La base de chaque prestation de service de cloud est constituée par les serveurs. Ceux-ci représentent l'équipement informatique sur lequel sont mises en place toutes les variations de services. Le modèle IaaS

constitue la variante de base parmi les services de cloud. Il est mis à disposition par des machines virtuelles («*virtual machines*») pour lesquelles l'utilisateur peut choisir non seulement la configuration souhaitée mais également le type de service (p. ex. calcul, enregistrement ou accès au réseau). Une machine virtuelle est une abstraction logicielle d'un serveur physique, qui met à disposition l'environnement nécessaire pour l'exploitation des applications utilisateur. Dans le cadre du modèle IaaS, l'utilisateur peut demander une ou plusieurs machines virtuelles, qui sont hébergées sur un ou plusieurs serveurs du fournisseur de services de cloud (cf. équipement informatique, selon l'illustration 2).

Le modèle PaaS peut être proposé sous deux formes: (1) en tant que plate-forme qui contient la structure de support et de gestion des applications de cloud, soit, typiquement, des outils de développement et de maintenance ainsi que d'actualisation des applications, ou (2) en tant que plate-forme en combinaison avec une infrastructure (IaaS) qui héberge les applications développées.

Les services Saas peuvent quant à eux être proposés sous trois formes: (1) uniquement l'hébergement («*hosting*») d'une application, (2) l'hébergement d'une application en combinaison avec PaaS, ou (3) l'hébergement d'une application en combinaison entre PaaS et IaaS.

Ces trois modèles de services caractérisent l'offre au sein de chaque niveau d'abstraction du service de cloud et rendent possibles des modèles de services plus spécifiques pour une ou plusieurs de ces trois catégories de services. En outre, ces modèles de services ainsi que les ressources nécessaires peuvent (tel que cela est présenté dans l'illustration 2) être combinés de différentes manières. Corollairement, il est possible de se voir mettre à disposition un service de cloud sur la base d'un autre service de cloud ou d'une certaine infrastructure.

2.1 Software-as-a-Service (SaaS)

Le modèle de services Software-as-a-Service (SaaS) met à disposition un service de «*cloud computing*»,

soit une application conviviale pour l'utilisateur final, basée sur le web. Dans ce modèle, un cabinet d'avocats ne gère ou ne contrôle pas les services de base mais uniquement les applications (p. ex. sous forme de traitement de texte, de transparents pour les présentations ou de programme de facturation). Tous les logiciels et données en relation sont enregistrés de manière centralisée dans l'infrastructure cloud, ce qui facilite la gestion du cloud et le support fourni autour des applications.

2.2 Platform-as-a-Service (PaaS)

Dans le modèle de services PaaS, le fournisseur de services de cloud met à la disposition des utilisateurs l'équipement informatique et les outils de développement pour l'élaboration, les tests et la mise à disposition des applications. Le but de ce modèle est de réduire les coûts et la complexité du matériel informatique utilisé en aval. Les applications PaaS sont en principe développées exclusivement sur mesure pour le prestataire de PaaS, de telle sorte que ces applications ne peuvent être proposées que via la plate-forme du fournisseur de services de cloud, ce qui entraîne un effet de blocage («*lock-in*»).

Le modèle de services PaaS est utilisé pour développer des applications, raison pour laquelle on part du principe, à l'heure actuelle, que les cabinets d'avocats n'utilisent pas ce modèle. Il est en revanche possible que des fournisseurs de logiciels fassent appel à un modèle PaaS.

2.3 Infrastructure-as-a-Service (IaaS)

Dans le modèle de service IaaS, les ressources de cloud computing (par ex. le calcul, le stockage ou l'accès au réseau) sont mises à disposition en tant que service. Le modèle IaaS constitue le modèle de base

des prestations de cloud. Il représente une option intéressante pour les entreprises à la recherche d'une infrastructure informatique incluant des ordinateurs, comme p. ex. un centre de calcul, mais qui, pour des raisons de coûts, ne peuvent pas l'exploiter elles-mêmes. Les coûts de maintenance élevés pour les centres de calcul ainsi que la demande de solutions moins onéreuses ont entraîné l'augmentation du nombre de prestataires spécialisés en IaaS qui prennent en charge, selon les besoins, la maintenance ainsi que des tâches de gestion (mise à disposition d'un site physique, climatisation, connectivité, électricité, réseau, sécurité physique et logique), ce qui permet à l'utilisateur de se concentrer davantage sur son domaine.

Le modèle IaaS est intéressant pour les cabinets d'avocats qui souhaitent utiliser des logiciels qui ne sont pas proposés dans le cadre du modèle de services SaaS et qui préfèrent ne pas devoir gérer eux-mêmes une infrastructure informatisée. Ainsi, p. ex., un cabinet d'avocats peut utiliser chaque logiciel y compris le système d'exploitation, sans devoir contrôler ou gérer l'infrastructure de base du cloud.

3. Mesures de sécurité dans le modèle de cloud

Les cabinets d'avocats qui sont intéressés à une solution de cloud ont le choix entre différents modèles de cloud. Un cabinet d'avocats peut louer uniquement une infrastructure (IaaS) et utiliser la mémoire dédiée, ou louer une solution de mémoire en nuage informatique complète afin d'être libéré des détails techniques (scénario 1). Ce modèle est idéal si l'on cherche uniquement à stocker des données. Cependant, les cabinets d'avocats pourraient également être intéressés à un traitement de données basé sur un nuage informatique. Dans ce cas, ils peuvent acquérir des solutions en nuage (SaaS) incluant des tableurs ou des logiciels de traitement de texte, de création de transparents pour les présentations, ou de facturation pour les documents enregistrés dans le cloud (scénario 2). Ce faisant, il est possible de choisir entre une application sur mesure et une application standard («*commercial off-the-shelf*»).

3.1 Mesures de sécurité SaaS, PaaS et IaaS

Le choix du modèle de services influe considérablement sur les mesures de sécurité («*security measures*») requises. L'illustration 3 présente cette connexité.

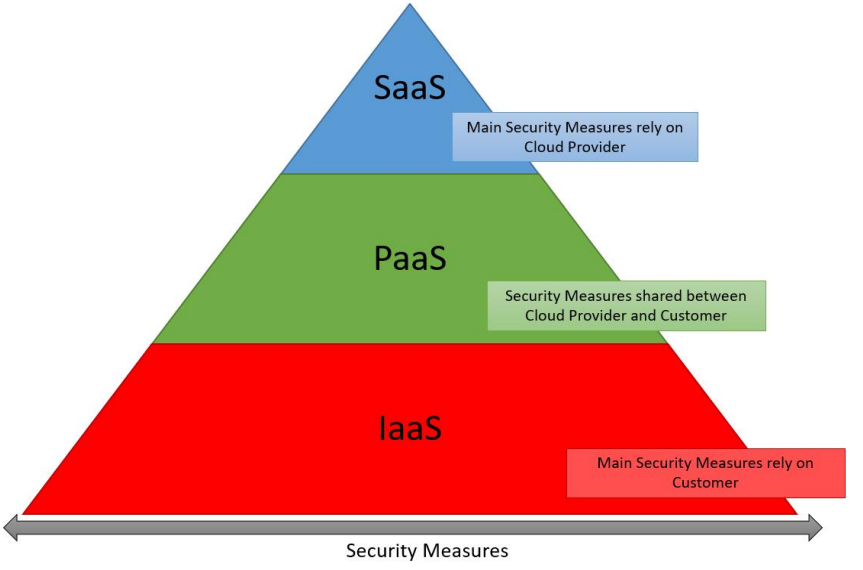

Illustration 3: modèles de services de cloud et responsabilité en matière de sécurité

a) IaaS

Le fournisseur de services de cloud met à la disposition du client une ou plusieurs machines virtuelles. L'ensemble de la configuration ainsi que la gestion des applications relatives à l'infrastructure mise à disposition restent de la responsabilité du client. Par suite, la plupart des mesures relatives à la confidentialité et à l'intégrité sont prises dans le cadre de la configuration par le client. Cependant, il s'agit de tenir compte du fait que, d'un point de vue technique, le fournisseur de services de cloud est responsable du fait que les données enregistrées sur les machines virtuelles ne puissent pas être consultés par d'autres utilisateurs via leurs machines virtuelles ou par le fournisseur lui-même (confidentialité) et que l'ayant droit puisse consulter ses données en tout temps (disponibilité).

b) PaaS

Dans le cadre du modèle de services PaaS, la responsabilité pour la sécurité est partagée, étant donné que le fournisseur de services de cloud met à disposition l'infrastructure ainsi que la plate-forme et que l'utilisateur est libre de configurer l'environnement du cloud selon ses exigences. Le fournisseur de services de cloud est responsable du fait que, dans le cadre de l'infrastructure, les données et la configuration du client demeurent confidentielles et disponibles en tout temps pour le client. Le client est cependant responsable de la configuration de la plate-forme et des aspects de sécurité.

c) SaaS

Contrairement à ce qui est le cas pour les modèles IaaS et Paas, la responsabilité de l'utilisateur en matière de sécurité est minime dans le cadre du modèle de services SaaS. Ici en effet, la responsabilité de l'utilisateur se limite à la sécurité des données d'accès. Le fournisseur de services de cloud est en revanche responsable de la confidentialité des données, de l'intégrité du réseau et de la disponibilité des services.

3.2 Scénario 1

L'illustration 4 présente deux mises en place possibles de modèles d'enregistrement de cloud. Dans la moitié supérieure de l'illustration, l'enregistrement des données n'est plus entrepris localement au sein du cabinet d'avocats, mais par un fournisseur de services de cloud. La transmission par le réseau se fait de manière sécurisée – c'est-à-dire au moyen de données cryptées – en utilisant un protocole HTTPS (Hypertext Transfer Protocol Secure) avec utilisation de TLS (Transport Layer Security), qui recourt à un cryptage fort (128 bit) ou très fort (256 bit). TLS est la version actualisée de SSL (Secure Socket

Layer) 3.0[1]. Toute communication qui dépend de HTTPS doit faire appel à TLS en tant que protocole cryptographique. Les données parviennent au fournisseur de services de cloud sous forme de paquets IP (protocole internet) cryptés avant la transmission. Dès que le fournisseur de services de cloud dépose ces paquets IP au sein de son infrastructure locale, les données sont cryptées au moyen d'une clé cryptographique locale du fournisseur de services de cloud, p. ex. au moyen de l'algorithme de chiffrement AES (Advanced Encryption Standard).

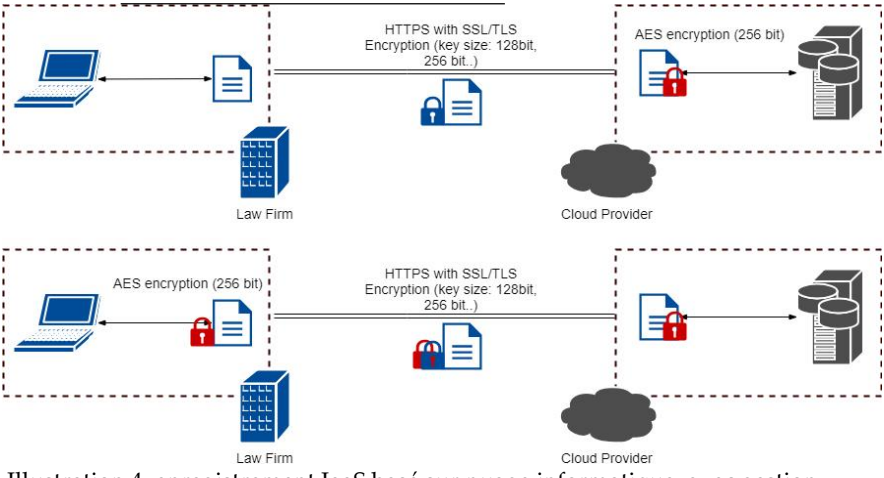

Illustration 4: enregistrement IaaS basé sur nuage informatique, avec gestion alternative des clés

La moitié inférieure de l'illustration 4 montre que les données destinées à être enregistrées auprès du fournisseur de services de cloud peuvent être cryptées par le cabinet d'avocats avant même la transmission via le réseau. Ce faisant, seul le cabinet d'avocats peut accéder aux données, celui-ci étant le seul à disposer des clés. Dans ce cas, le cabinet d'avocats ne place pas sa confiance dans le cryptage du

[1] SSL 3.0 a été classée obsolète par l'Internet Engineering Task Force (IETF) dans le document RFC 7568.

fournisseur de communications, mais sur celui du fournisseur de services de cloud, tout en y faisant recours lui-même. Les étapes restantes nécessaires à la transmission cryptée et à l'enregistrement par le fournisseur de services de cloud demeurent les mêmes, avec pour seule différence que le fournisseur de services de cloud ne doit plus crypter les données avant l'enregistrement. Pendant la transmission, les données sont doublement protégées, soit d'une part au moyen de la clé du cabinet d'avocats, et d'autre part au moyen de la clé HTTPS SSL/TLS.

Le cloud computing – et notamment l'enregistrement de données dans un nuage informatique («*cloud storage*») – n'apporte pas que des avantages, la combinaison entre différentes technologies ayant également des points faibles. Ainsi, p. ex., les mécanismes de virtualisation couramment employés n'ont pas été développés spécialement pour l'informatique en nuage, mais ont été adaptés au cloud computing afin de maximiser les ressources disponibles. Tout comme l'enregistrement et le traitement de données tels que pratiqués usuellement – soit p. ex. en enfermant des documents dans un coffre-fort ou en enregistrant et en traitant des données sur un ordinateur autonome –, l'utilisation de services de cloud est liée à un certain nombre de risques. Afin de minimiser ces risques, des mesures de sécurité spécifiques doivent être prévues en tenant compte du type d'attaque à craindre ou du risque existant.

3.3 Scénario 2

Selon le scénario 2 présenté à l'illustration 5, un cabinet d'avocats recourt à des applications de traitement de textes ou de préparation de présentations selon le modèle SaaS. Dans le cadre d'un tel modèle, le fournisseur de services de cloud gère le logiciel dans une machine virtuelle («*hosting*») pour le cabinet d'avocats. Les données sont ainsi transférées de manière cryptée via HTTPS avec SSL/TLS, entre le cabinet d'avocats et le fournisseur de services de cloud. Ces données ne sont cependant pas des données ou des documents comme dans le

scénario 1, mais des informations sur les actions entreprises par l'utilisateur au niveau du logiciel (p. ex. copier, insérer, éditer, créer un nouveau document, enregistrer). Après l'enregistrement, le document est crypté et archivé par le logiciel du fournisseur de services de cloud au moyen d'une clé cryptographique différente pour chaque utilisateur. Ce faisant, il importe de considérer dans ce modèle SaaS que, du point de vue technique, le fournisseur de services de cloud a accès aux données enregistrées dans le document. D'autres utilisateurs du nuage informatique ne disposent en revanche d'aucune possibilité d'accès, parce que les documents sont cryptés au moyen de clés différentes, ce qui garantit l'isolement des données. Le contenu des fichiers est par suite visible pour le fournisseur de services de cloud, mais non pour les autres clients de ce fournisseur qui utilisent également ce service. Les clients du fournisseur de services de cloud qui traitent des données confidentielles doivent être conscients du fait que dans le cadre du modèle SaaS, le fournisseur pourrait aussi utiliser ces données. Par suite, de telles prestations de service doivent, sous l'angle technique, être considérées avec retenue, et des mesures de précaution adéquates doivent être prises.

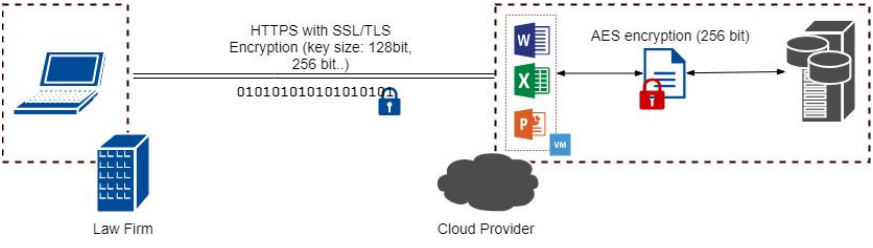

Illustration 5: fournisseur de services de cloud SaaS disposant de propres mécanismes de sécurité

III. Droit pénal

La question de savoir si les avocates et avocats se rendent punissables si, dans le cadre de l'exercice de leur profession, elles/ils utilisent les services d'un fournisseur de services de cloud pour le traitement de données doit être en premier lieu examinée à l'aune des éléments constitutifs de la violation du secret professionnel (art. 321 CP). Pour ce faire, il s'agit de prendre en considération parallèlement les éléments constitutifs de l'infraction au droit de la protection des données, à savoir la violation du devoir de discrétion (art. 35 LPD), et la réglementation du secret professionnel des avocates et avocats (art. 13 LLCA). Sous l'angle du droit pénal, la question centrale est de savoir si le fait d'enregistrer et de traiter des données au sein d'un nuage informatique constitue une divulgation illicite d'un secret professionnel. Dans ce cadre, il s'agit en particulier de clarifier, d'une part, si les fournisseurs de services de cloud doivent être qualifiés d'auxiliaires au sens du droit pénal et, d'autre part, si la divulgation d'un secret professionnel à un(e) auxiliaire constitue un élément constitutif de l'infraction.

1. Violation du secret professionnel (art. 321 CP)

1.1 Type de délit

Les dispositions pénales de la partie spéciale du code pénal (CP) sont classées selon différents types de délits, au vu des éléments objectifs de l'infraction. En premier lieu, on distingue selon le moment auquel l'élément constitutif de l'infraction est donné. Pour les délits de mise en danger abstraite, le moment de la consommation du délit est placé très en amont et est déjà atteint lorsqu'un acte que le législateur qualifie de manière générale – donc abstraite – de mise en danger[2] est ac-

[2] Exemple: lorsque la pornographie est rendue accessible, les éléments objectifs de l'infraction selon l'art. 197 al. 1 CP sont déjà donnés lorsque la consultation, respectivement la visualisation par une personne quelconque âgée de moins de

compli. Pour les délits de mise en danger concrète, au moins un titulaire d'un bien juridique ou un objet juridique doit être mis en danger de manière avérée. Pour ce type de délits, le comportement punissable ne suffit donc pas: une mise en danger concrète doit en outre avoir lieu pour le titulaire du bien juridique protégé[3]. La plupart des éléments constitutifs de l'infraction doivent représenter davantage qu'une simple mise en danger du bien juridique ou du titulaire de ce bien. Pour que l'infraction soit consommée, on doit en effet être en présence de la violation d'un droit[4]. Une autre différenciation classe les éléments constitutifs de l'infraction en délits formels, d'une part, et délits matériels (ou «de résultat»), d'autre part. Selon la doctrine de droit pénal, il suffit que l'acte incriminé ait été accompli pour que le délit formel soit réputé consommé. Pour les délits matériels, l'acte perpétré doit en outre entraîner un résultat. Des recoupements existent entre les éléments distinctifs, mais tous les délits de mise en danger abstraite sont considérés comme des délits formels (simples) parce que le délit est déjà consommé lors de la simple exécution de l'acte[5]. Ces distinctions sont importantes non seulement pour délimiter la tentative de la consommation et pour déterminer les éléments objectifs de l'infraction pour lesquels la preuve doit être apportée dans le

16 ans est possible, p. ex. lorsqu'un fichier pornographique est enregistré sur un site Internet librement accessible. La notion de délit de mise en danger «abstraite» est contradictoire; cf. SCHWARZENEGGER, sic! 2001, 247 et les réf. cit.

3 Exemple: si un auteur rédige une lettre qui renferme des accusations infamantes, les éléments constitutifs de la diffamation ou de la calomnie ne sont pas encore donnés. En effet, la perception d'un tiers quelconque doit intervenir pour que les éléments objectifs de l'infraction soient donnés (cf. art. 173 s. CP). Cela signifie que la lettre doit avoir été expédiée au destinataire et lue par lui. L'honneur de la personne concernée n'est mis en danger concrètement qu'à ce moment-là.

4 Exemple: il ne suffit pas de tirer sur une personne (mise en danger concrète): la mort de la victime doit en effet s'ensuivre pour que l'infraction de meurtre soit objectivement consommée (art. 111 CP).

5 Consulter, au sujet de ces distinctions dans le contexte d'Internet: SCHWARZENEGGER, E-Commerce, 346 ss et les réf. cit.

cadre de la procédure pénale, mais en particulier aussi pour définir le droit de la peine applicable (cf. art. 3 ss CP)[6].

L'art. 321 CP, selon lequel la violation du secret professionnel n'est poursuivie que sur plainte, protège en premier lieu le droit subjectif du maître du secret[7]. Cet aspect est confirmé par le ch. 2, qui prévoit la possibilité d'exclure la punissabilité par voie de consentement ou d'autorisation justifiée[8]. Le secret professionnel au sens du droit pénal n'englobe cependant pas toutes les relations existant entre une catégorie de professionnels et leurs clients, mais uniquement celles «pour lesquelles il existe un intérêt public à ce que le client puisse se confier sans réserve au professionnel»[9]. Dans ce sens, la norme pénale découle en outre indirectement de l'intérêt public à la protection de la relation de confiance particulière, parce que ce n'est que sur la base de la confidentialité que la profession d'avocat peut être exercée de ma-

---

6 Selon la doctrine dominante, le principe de la territorialité, qui est en première ligne déterminant pour la juridiction pénale, ne vaut, pour les délits purement formels et les délits de mise en danger abstraite, que pour le lieu de commission de l'acte (voir ci-dessous sous III.1.6).

7 Cela se laisse déjà déduire des travaux préparatoires: Expertenkommission I, vol. 2, Berne 1896, 14, «*Verletzung in den persönlichen Verhältnissen des Betroffenen*»; ZÜRCHER, Protokoll der zweiten Expertenkommission Strafgesetzbuch, 364, le secret privé du maître du secret («*das private Geheimnis des Geheimnisinhabers*») est protégé. Donc pas le droit du détenteur du secret, voir NIGGLI, Gutachten Unternehmensjuristen, 17, 32 et les réf. cit., «*Geheimsphäre des Berechtigten*»; PK-StGB, TRECHSEL/VEST, StGB 321 N 1 et les réf. cit., selon lequel le CP a rejoint cette position («*dieser Richtung angeschlossen*»).

8 L'art. 321 ch. 2 CP parle du consentement de l'intéressé. À la différence du consentement, qui a un effet justificatif, on parle d'accord lorsque l'illicéité est un élément constitutif de la définition générale et abstraite du tort causé et que l'accord suffit déjà à faire tomber la typicité de l'infraction. Cette différenciation revêt une signification dans la mesure où dans le dernier cas, l'intention doit également comprendre l'illicéité. Voir l'exemple relatif aux dispositions pénales en matière de droit d'auteur, SCHWARZENEGGER, RDS 2008 II, 467 et les réf. cit.

9 BSK-Strafrecht II, OBERHOLZER, StGB 321 N 4.

nière correcte et irréprochable[10]. Mais cela ne change rien au fait que cette disposition pénale soit conçue comme sanctionnant un délit contre un bien juridique individuel. L'intérêt public se manifeste uniquement en rapport avec la limitation au groupe de professions citées[11].

La conception des délits de mise en danger abstraite est destinée à protéger l'intérêt public. Leur consommation commence dès le moment du comportement répréhensible (anticipation du caractère délictueux), soit à un moment auquel le titulaire du bien juridique, qui pourra être déterminé plus tard, n'est pas encore connu. De ce fait, il s'agit d'infractions poursuivies d'office[12]. Il en résulte que la violation du secret professionnel selon l'art. 321 ch. 1 premier alinéa CP ne peut pas être un délit de mise en danger abstraite. Selon la jurisprudence du Tribunal fédéral et la doctrine dominante, la prise de connaissance par un tiers est présupposée pour la consommation del'acte[13]. Cela signifie qu'une violation du secret matériel constitue une condition préalable à la réalisation des éléments objectifs de l'infraction. Cependant, cette caractérisation ne s'accorde pas avec la formulation souvent répétée que l'on est en présence d'un acte délictueux lorsque l'auteur de l'infraction divulgue le secret à un tiers non autorisé à connaître ce secret ou qu'il «rend du moins possible cette prise de connaissance»[14]. Aussi, les éléments de l'infraction ne peuvent être

---

10 ATF 112 Ib 606, consid. b. Comp. PK-StGB, TRECHSEL/VEST, StGB 321 N 1 et les réf. cit.

11 De même, NIGGLI, Gutachten Unternehmensjuristen, 32 et les réf. cit.

12 SCHMID, § 5 N 11 avec les réf.; SCHWARZENEGGER, RDS 2008 II, 464 s.

13 ATF 6B_1403/2017 du 8 août 2017, consid. 1.2.2; ISENRING, StGB/JStGB-Kommentar, StGB 321 N 10b; DONATSCH/THOMMEN/WOHLERS, 580 s.; BSK-Strafrecht II, NIGGLI/HAGENSTEIN, StGB 162 N 36; BSK-Strafrecht II, OBERHOLZER, StGB 320 N 10.

14 ATF 142 IV 65, consid. 5.1; BSK-Strafrecht II, OBERHOLZER, StGB 320 N 10. TF, arrêt 6B_1403/2017 du 8 août 2017, consid. 1.2.2, «*Es handelt sich hierbei um eine blosse Umschreibung des strafbaren Verhaltens, woraus – entgegen der Meinung der Vorinstanz – nichts zum Zeitpunkt der Vollendung der Tat abgeleitet werden kann. Vielmehr ist in dieser Frage der Lehre zu folgen, wonach die Tat vollendet ist, sobald ein Aus-*

donnés uniquement du fait d'un archivage insuffisant des informations secrètes[15]. Selon la doctrine dominante, l'art. 321 ch. 1 premier alinéa CP réprime une infraction de lésion. Les éléments objectifs de l'infraction de l'art. 321 ch. 1 premier alinéa CP sont donnés dès que le détenteur du secret au sens de l'art. 321 ch. 1 premier alinéa CP cause, par action ou par omission, la prise de connaissance du secret par au moins un tiers non autorisé[16]. Étant donné que la prise de connaissance du secret constitue un effet extérieur particulier causé par le comportement délictueux, on se trouve en même temps, pour l'art. 321 ch. 1 premier alinéa CP, en présence d'un délit de résultat.

En bref, on retiendra que la violation du secret professionnel au sens de l'art. 321 CP vient se ranger parmi les infractions contre un bien juridique individuel. Le délit est à la fois un délit de lésion et un délit de résultat.

1.2 Éléments objectifs de l'infraction

a) Objet de l'atteinte: le secret protégé

L'objet de l'atteinte dans le cadre de la violation du secret professionnel est un secret que l'auteur du délit s'est vu confier en raison de sa profession ou qui a été porté à sa connaissance dans le cadre de l'exercice de sa profession. Les secrets matériels sont protégés par la loi. Un secret doit ainsi être une information relativement inconnue, et

senstehender dank dem Verhalten des Täters Kenntnis vom betreffenden Geheimnis erhält». Cette motivation constitue une *petitio principii* et ne convainc pas.

15 Voir cependant BSK-Strafrecht II, OBERHOLZER, StGB 321 N 19; STRATENWERTH/BOMMER, § 61 N 19; PK-StGB, TRECHSEL/VEST, StGB 321 N 23, ce qui plaiderait plutôt en faveur d'un délit de mise en danger concrète. Si l'accomplissement de l'acte requiert au minimum la prise de connaissance par un tiers non autorisé, alors la conservation insuffisante est en soi tout au plus punissable au titre de tentative de violation du secret professionnel.

16 Ainsi déjà GAUTIER, Expertenkommission II, vol. IV, Lucerne 1915, p. 365 «consommé par la révélation».

le maître du secret doit avoir un intérêt légitime à ce que l'information soit tenue confidentielle[17].

i. Caractère relativement inconnu

L'information est relativement inconnue lorsque seul un nombre limité de personnes disposent de l'information en question. N'est donc pas décisif le fait qu'une tierce personne prenne effectivement connaissance de l'information.

Est également protégée par le secret professionnel une information que le destinataire possédait ou supposait déjà, du fait que ses connaissances peu fondées ou incomplètes se trouveraient ainsi renforcées ou complétées par sa divulgation[18].

ii. Secret matériel

Dans la notion de secret matériel, l'intérêt du maître du secret est mis au premier plan[19]. Le maître du secret doit garder le contrôle sur la divulgation de l'information à des tiers, même s'il en parle avec un avocat ou un membre des autres professions énumérées à l'art. 321 ch. 1 premier alinéa CP. Le secret professionnel crée ainsi une relation de confiance qui doit permettre à l'avocat de clarifier de manière amplective les faits, conseiller correctement son client et lui permettre de faire valoir ses droits[20]. Ne tombent pas sous le coup du secret professionnel au sens de l'art. 321 ch. 1 premier alinéa 1 CP les informations

17 ATF 127 IV 122, consid. 1 et ATF 142 IV 65, consid. 5.1, tous deux avec les réf. cit. (concernant l'art. 320 CP); NIGGLI, Gutachten Unternehmensjuristen, 20 ss et les réf. cit.; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 14; STRATENWERTH/BOMMER, § 61 N 5; PK-StGB, TRECHSEL/VEST, StGB 321 N 20 ss et les réf. cit.

18 BSK-Strafrecht II, OBERHOLZER, StGB 321 N 19 STRATENWERTH/BOMMER, § 61 N 7; ATF 75 IV 71, consid. 1; FELLMANN, N 542.

19 NIGGLI, Revue de l'avocat 2006, 279 et les réf. cit.; STRATENWERTH/BOMMER, § 61 N 5, 15; DONATSCH/THOMMEN/WOHLERS, 587; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 1; ainsi déjà ZÜRCHER, Protokoll der zweiten Expertenkommission Strafgesetzbuch, 364.

20 Cf. BSK-Strafrecht II, OBERHOLZER, StGB 321 N 2; WOHLERS/LYNN, recht 2018, 12.

issues de ladite activité professionnelle accessoire de l'avocat, soit de la gestion de patrimoine, d'opérations de dépôt, de mandats de recouvrement ou de mandats de conseiller d'administration[21], ou encore de la vie privée de l'avocat.

L'art. 321 CP englobe toutes les informations qui ont été confiées à l'avocat en raison de sa profession ainsi que toutes les informations dont il prend connaissance dans le cadre de l'exercice de sa profession. L'art. 321 CP ne limite pas les informations à celles concernant le client et, vice versa, n'exige pas non plus que l'information ait été communiquée ou transmise sciemment à l'avocat[22]. Ainsi, le secret protégé peut également émaner d'un tiers, qui en est par suite le maître. Le rapport de causalité avec l'exercice du mandat est seul décisif[23].

Dans le cadre de cet avis de droit, nous n'examinerons pas plus avant la question de la qualité du secret. Il est incontesté que l'externalisation de données d'un client pose la question du respect du secret professionnel.

---

21 Cf. ATF 143 IV 462 consid. 2.2; NIGGLI, Gutachten Unternehmensjuristen, 21 ss; PK-StGB, TRECHSEL/VEST, StGB 321 321 N 21. La protection pénale ne vise que l'activité typique de l'avocat, mais il est parfois difficile de la circonscrire en pratique (concernant l'externalisation de tâches de compliance selon la LBA à un cabinet d'avocats, voir TF, arrêt 1B_85/2016 du 20 septembre 2016, consid. 6).

22 Ainsi déjà GAUTIER, Protokoll der zweiten Expertenkommission Strafgesetzbuch, 365; NIGGLI, Revue de l'avocat 2006, 279; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 16; PK-StGB, TRECHSEL/VEST, StGB 321 N 21 s.

23 Cf. ATF 115 Ia 197, consid. 3.c, selon lequel l'obligation de garder le secret à laquelle est soumis l'avocat ou l'avocate ne concerne que les faits qui lui ont été confiés par son client pour lui permettre d'exercer son mandat ou dont il a pris connaissance dans le cadre de l'exercice de son mandat (dans le même sens, ATF 112 Ib 606, consid. b). FELLMANN, N 559 s.

b) Cercle des auteurs de l'infraction: maître du secret et auxiliaires

La violation du secret professionnel au sens de l'art. 321 CP doit être qualifiée de délit spécial proprement dit, ce qui signifie que seuls les professionnels explicitement et exhaustivement énumérés dans la disposition peuvent en être les auteurs[24]. Les avocates et avocats, mais aussi leurs auxiliaires, sont nommés à l'art. 321 ch. 1 premier alinéa CP et sont de ce fait punissables[25]. La catégorie des avocats comprend toutes les personnes qui ont suivi une formation professionnelle correspondante et qui sont titulaires d'un certificat de compétence suisse ou étranger, qu'elles pratiquent ou non dans le cadre du monopole[26]. L'inscription au registre cantonal des avocats n'est pas non plus déterminante. La question de savoir si seuls les avocats indépendants ou également les juristes d'entreprise sont soumis au secret professionnel de l'avocat est contestée[27]. Vu le fait que selon le CPP, la défense des prévenus est réservée aux avocats qui, en vertu de la LLCA, sont habilités à représenter les parties devant les tribunaux (art. 2 LLCA, art. 127 al. 5 CPP; exception: défense dans le cadre des procédures pénales en matière de contraventions), la mention explicite des défenseurs à l'art. 321 ch. 1 premier alinéa CP ne revêt plus guère de signi-

---

24 ZÜRCHER, 351; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 11; PK-StGB, TRECHSEL/VEST, StGB 321 N 3; STRATENWERTH/BOMMER, § 61 N 17.

25 BSK-Strafrecht II, OBERHOLZER, StGB 321 N 4; PK-StGB, TRECHSEL/VEST, StGB 321 N 5; BOHNET/MARTENET, 741.

26 NIGGLI, Gutachten Unternehmensjuristen, 15, 19 s.

27 Cf. BSK-Strafrecht II, OBERHOLZER, StGB 321 N 6; PK-StGB, TRECHSEL/VEST, StGB 321 N 5, qui considèrent que les juristes d'entreprise ne sont pas inclus; voir également, concernant cette controverse: NIGGLI, Gutachten Unternehmensjuristen, *passim*; PFEIFER, Revue de l'avocat 2006, 166 ss; NIGGLI, Revue de l'avocat 2006, 277 ss.

fication particulière. La disposition englobe également les notaires et les conseils en brevets ainsi que d'autres groupes de professions[28].

Ce qui est décisif en l'espèce, c'est l'interprétation de la notion d'auxiliaire d'une personne appartenant à un groupe professionnel soumis à l'obligation de garder le secret professionnel. La doctrine et la jurisprudence citent parmi les auxiliaires[29]: les assistants, les secrétaires, les bureaux d'administration externes («secrétariat délocalisé»)[30], le personnel de cabinet d'avocat, les stagiaires, les comptables, les détectives privés[31], les experts, tous les collaborateurs au sein d'une équipe placée sous les ordres d'un médecin (psychologues, pédagogues, assistants sociaux, aides-soignants, thérapeutes, personnel de laboratoire), le personnel soignant, les assistants médicaux, le personnel auxiliaire subordonné, dans la mesure où il entre en contact avec des informations sur les patients, les prothésistes dentaires[32], les sages-femmes (dans la mesure où elles sont soumises aux ordres d'un médecin[33]) ainsi que les membres du personnel de nettoyage et de la centrale téléphonique, dans la mesure où ils entrent en contact avec des informations concernant le maître du secret[34].

---

28 Pour plus de précisions concernant les différents groupes de professions, cf. BSK-Strafrecht II, OBERHOLZER, StGB 321 N 5 ss; PK-StGB, TRECHSEL/VEST, StGB 321 N 6 ss.

29 BezGer Zürich, arrêt du 18 novembre 2015, GG 150233, consid. II.2.5.3; BLATTMANN, in: Baeriswyl/Rudin, IDG 6 N 10; DONATSCH/THOMMEN/WOHLERS, 590; KELLER, 107; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 10; STOCKER, ZStrR 1953, 9; PK-StGB, TRECHSEL/VEST, StGB 321 N 13; cf. ég. TF, arrêt 1B_447/2015 du 25 avril 2016, consid. 2.2.

30 BezGer Zürich, arrêt du 18 novembre 2015, GG 150233, consid. II.2.5.5.

31 TF, arrêt 1B_447/2015 du 25 avril 2016, consid. 2.2; CORBOZ, CP 321 N 16; FELLMANN, N 555; CR-LLCA, MAURER/GROSS, LLCA 13 N 97.

32 PK-StGB, TRECHSEL/VEST, StGB 321 N 10.

33 PK-StGB, TRECHSEL/VEST, StGB 321 N 12.

34 PK-StGB, TRECHSEL/VEST, StGB 321 N 13; REHBERG, 340 s. Concernant cette catégorie, d'un autre avis: STRATENWERTH/BOMMER, § 61 N 17, non convaincants. Si le personnel de nettoyage est compté parmi les tiers non autorisés, l'avocat (ou l'avocate) doit obtenir l'autorisation préalable du maître du secret, c'est-à-dire

Certains auteurs sont d'avis que les membres du personnel chargé de la maintenance des installations techniques ne peuvent pas être qualifiés d'auxiliaires au sens de l'art. 321 CP[35]. Nous ne pouvons approuver cet avis de manière globale. Il s'agit plutôt d'examiner, comme pour le personnel de nettoyage, si le personnel chargé de la maintenance prend connaissance d'informations sur les clientes et clients de l'avocat, dans le cadre de cette fonction. S'agissant de la maintenance des installations de chauffage au sein d'un cabinet d'avocats par un concierge, on ne saurait qualifier celui-ci d'auxiliaire, car il n'est pas chargé de traiter des documents. En revanche, les spécialistes en informatique mandatés ou employés qui sont chargés d'apporter leur soutien à l'avocat dans la gestion et l'archivage des données ainsi que dans l'utilisation des logiciels sont clairement actifs dans un domaine d'activités qui implique forcément la prise de connaissance d'informations confidentielles[36]. Contrairement à ce qui était le cas autrefois alors que la gestion des documents avait encore lieu sous forme papier, le support informatique constitue de nos jours l'une des fonctions d'aide centrales en matière de traitement numérique des informations et de gestion des documents. Ceci est également valable au sein des cabinet d'avocats. Le spécialiste en informatique, respectivement les collaborateurs du fournisseur de services informatiques en charge de l'infrastructure informatique et des applications, entrent ainsi dans la catégorie des auxiliaires[37].

avant que le personnel de nettoyage soit autorisé à nettoyer les locaux administratifs, à défaut de quoi l'avocat devra nettoyer lui-même les bureaux afin d'écarter le risque de punissabilité selon l'art. 321 CP.

35 PK-StGB, TRECHSEL/VEST, StGB 321 N 13 et les réf. cit. de LANGMACK, ZStrR 1972, 67; ROSSEL, SZS 1992, 243 s., s'agissant d'auxiliaires de médecins.

36 Ceci vaut également pour le personnel informatique interne, cf. WOHLERS, 23.

37 De manière similaire concernant l'organisation interne des banques selon les tâches (en lien avec l'art. 47 LB), cf. ALTHAUS STÄMPFLI, 143, qui présente explicitement le service «informatique» comme constitué par les «*Personen, welche einen Beitrag an die vom Kunden gewünschten Dienstleistungen erbringen*».

L'auxiliaire au sens de l'art. 321 ch. 1 premier alinéa CP est soumis à la même obligation de traiter de manière confidentielle les informations qui lui sont confiées dans le cadre de son activité pour le détenteur (principal) du secret ou qui parviennent à sa connaissance dans le cadre de cette activité, que celle à laquelle est soumis le détenteur (principal) du secret. Deux conséquences importantes en découlent sur la base de l'interprétation grammaticale, systématique, historique et téléologique de la loi (i et ii). En outre, il s'agit d'examiner plus en détail les formes d'organisation du travail lorsque plusieurs détenteurs (principaux) du secret travaillent côte à côte (iii).

i. Définition fonctionnelle de l'auxiliaire

Selon l'interprétation grammaticale, qui se base sur le sens, les auxiliaires (en allemand «*Hilfspersonen*» et en italien «*ausiliari*») sont des individus qui soutiennent une personne dans l'accomplissement d'une tâche. Le sens littéral couvre tous les types d'assistance, qu'il s'agisse de travaux de dactylographie, de recherche, de courses ou encore d'assistance à la saisie, au traitement et à l'archivage des données. De même, les bénéficiaires de services de sous-traitance qui mettent à la disposition du détenteur du secret un traitement des données efficace peuvent parfaitement tomber sous le coup de cette définition.

La règle d'interprétation systématique détermine le sens d'une norme en examinant sa relation avec d'autres normes et lois. Des indices d'interprétation peuvent même se trouver dans une disposition, notamment en cas d'énumération qui caractérise le cercle des auteurs d'une infraction ou les éventuels actes délictueux. Le fait qu'à l'art. 321 ch. 1 premier alinéa CP, les auxiliaires soient mentionnés dans la catégorie des détenteurs (principaux) du secret (en allemand: «*sowie* […]»; en français: «ainsi que […]»; en italien: «*come pure* […]») et soient soumis à la même menace de sanction, constitue un indice fort en faveur d'une volonté du législateur d'élargir le cercle des personnes qui prennent connaissance du secret, selon une conception fonctionnelle d'un environnement professionnel partagé. Si le législa-

teur avait voulu restreindre le cercle des auxiliaires, cela aurait dû transparaître du point de vue notionnel.

L'interprétation historique fournit également des indices clairs. Le législateur est parti du principe que les ecclésiastiques, les avocats, les défenseurs, les notaires, les conseils en brevets, etc. ne sont pas tenus d'exercer leur activité professionnelle seuls, mais qu'ils ont le droit de diviser leur travail[38]. Les travaux préparatoires montrent clairement qu'une conception étroite du cercle des auxiliaires a été explicitement rejetée. Les doutes soulevés par deux membres de la commission d'experts, qui préconisaient une notion plus restreinte, fut noté mais sciemment laissé de côté. Ainsi, ALFRED GAUTIER, en tant que membre de la seconde commission d'experts, attira l'attention sur les problèmes de délimitation: «Car il est délicat de délimiter le cercle de ces auxiliaires. On risque d'y comprendre de simples petits comparses sur lesquels ne doit reposer aucune responsabilité spéciale, […]»[39]. La commission d'experts ne s'est cependant pas étendue sur cet argument. Conformément à GAUTIER, EUGÈNE DESCHENAUX déposa une motion demandant que le terme d'«auxiliaire» soit remplacé par celui d'«assistant ou employé supérieur»[40]. Une vision très restrictive de la manière dont le secret devrait être conservé au sein d'un bureau y était liée: «… ou bien le patron met sous clef ce qui doit rester secret, ou bien c'est lui qui encourt la responsabilité pour ne s'être pas entouré d'un personnel suffisamment discret et réservé»[41]. Donc, le chef devrait, selon lui, tout mettre sous clef s'il veut écarter tout risque. La motion DESCHENAUX a été rejetée par la commission d'experts, à une

[38] PK-StGB, TRECHSEL/VEST, StGB 321 N 23 concernant la répartition du travail au sein d'équipes; cf. également WOHLERS, 21, qui reconnaît en principe la nécessité de répartir les tâches.

[39] Protokoll der zweiten Expertenkommission Strafgesetzbuch, 365.

[40] Protokoll der zweiten Expertenkommission Strafgesetzbuch, 371. Il s'agissait surtout, pour lui, d'exclure une éventuelle punissabilité des employés subordonnés.

[41] Protokoll der zweiten Expertenkommission Strafgesetzbuch, 372.

large majorité[42]. De même, lors des débats parlementaires portant sur la loi, la remarque du président de la commission du Conseil national selon laquelle la notion d'«auxiliaires de ces personnes» était quelque peu vague n'a conduit à aucun débat, ou à aucune délimitation de la notion, ni même à aucune adaptation de la disposition pénale[43].

D'un point de vue téléologique également, une limitation stricte du cercle des auxiliaires n'a aucun sens. Dans le cadre d'un environnement professionnel à tâches partagées, le nombre de personnes tierces non autorisées augmenterait ainsi automatiquement. En cas de définition restrictive de la notion, le détenteur du secret[44] serait personnellement tenu de tout mettre sous clé, sécuriser et crypter ainsi que de procéder à la maintenance des systèmes d'exploitation informatiques et de gérer les données – que les informations confidentielles soient traitées et classées sous forme papier ou sous forme de données numériques au niveau d'un ordinateur fixe local, d'un serveur réseau du cabinet d'avocats ou dans un nuage informatique –, afin de se prémunir contre tout éventuel accès par des tiers non autorisés, soit p. ex. par des membres du personnel de nettoyage, du secrétariat ou du service informatique. Cependant, cela ne saurait correspondre au sens et au but de la loi de contraindre des groupes professionnels hautement spécialisés à mettre en place de tels processus accablants, impossibles à mettre œuvre au sein de l'exploitation ou du moins hautement inefficients. La protection du secret professionnel et la préservation des intérêts du maître du secret sont au contraire suffisamment garanties du fait de la soumission des auxiliaires au secret professionnel et à la responsabilité civile ainsi qu'à la responsabilité relative au droit de surveillance du détenteur (principal) du secret. Celui-ci est

42 Protokoll der zweiten Expertenkommission Strafgesetzbuch, 376.

43 Stenographisches Bulletin, Nationalrat, 26.9.1929, p. 612. Avis divergent, sans interprétation propre ou prise en compte des travaux préparatoires, cf. SCHÄFER, 39 s.

44 Ainsi que le nombre restreint d'employés reconnus comme auxiliaires, comme p. ex. les stagiaires.

alors responsable de choisir ses auxiliaires avec soin et de les instruire en conséquence.

Les différentes approches d'interprétation aboutissent à un résultat clair et concordant: la protection du secret professionnel en Suisse entend l'auxiliaire de manière large et fonctionnelle[45]. Ainsi, l'auxiliaire est toute personne qui participe à l'activité professionnelle du détenteur (principal) du secret d'une manière telle qu'il lui est en principe possible d'accéder à des informations confidentielles. Il suffit pour cela que l'auxiliaire soutienne la personne principale tenue au secret professionnel dans l'exécution de ses tâches[46]. Il est permis de confier le traitement de données confidentielles à des auxiliaires dans la mesure où la loi ne l'interdit pas. Le secret professionnel au sens de l'art. 321 ch. 1 premier alinéa CP ne s'oppose pas à une organisation du travail du détenteur du secret professionnel qui soit judicieuse sur le plan économique. Les activités professionnelles courantes comme les travaux de secrétariat, les recherches, la gestion et l'archivage des dossiers, la commande et la mise en place de matériel, les courses à la Poste, etc. peuvent être confiées à des auxiliaires. Le même principe doit valoir pour le traitement électronique des données. L'installation et la maintenance des ordinateurs et programmes, la saisie électronique, le traitement et l'archivage de données, la maintenance à distance de l'équipement des utilisateurs, etc. ne peuvent de fait pas être assurés par le détenteur du secret à lui seul. Pour ces tâches, il est

---

45 BezGer Zürich, arrêt du 18 novembre 2015, GG 150233, consid. II.2.5.2, «*Der Kreis der Hilfspersonen ist praktisch unbegrenzt*»; CHAPPUIS/ALBERINI, Revue de l'avocat 2017, 339 s.; KELLER, 106 ss et les réf. cit., avec la restriction à la «*Berufsmässigkeit*»; NIGGLI, Gutachten Unternehmensjuristen 30 s.; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 10; PK-StGB, TRECHSEL/VEST, StGB 321 N 13; STRATENWERTH/BOMMER, § 61 N 17, avec la restriction à la «*Berufsmässigkeit*»; cf. NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 51 s. et N 53: «*Massgeblich ist vielmehr sowohl strafrechtlich als auch berufsrechtlich, ob die Tätigkeit der Hilfsperson die Möglichkeit des Zugangs zu geschützten Informationen einschliesst*».

46 D'un avis contraire, cependant sans interprétation propre et sans tenir compte des travaux préparatoires SCHÄFER, 39 s.; cf. ég. HAFTER, 854 s.; d'un avis contraire également WOHLERS, voir à ce sujet III.1.2b)iv.

tributaire du soutien de spécialistes[47], qui agissent sur la base de ses instructions et qui sont soumis à son contrôle. Même si, en relation avec le secret professionnel, on pense en premier lieu à la protection au sein des locaux administratifs du détenteur du secret – par analogie au bureau particulièrement sécurisé et aux archives à la cave[48] –, les activités menées en dehors de ces espaces protégés[49], voire même à l'étranger[50], sont depuis toujours possibles et inclues, comme p. ex. l'envoi et la réception de courrier postal, les interrogatoires ou entretiens avec les clients menés à l'extérieur, le transport d'informations protégées sous forme de copie papier, sur disque dur ou clé USB, etc. Les auxiliaires sont eux aussi autorisés à manier des informations

47 Voir, sous le point de vue contractuel: STRAUB, PJA 2014, 913: «*Wenn der Auftraggeber selbst nicht über die entsprechenden Kompetenzen verfügt, kann die Datensicherheit eine Auslagerung der Datenbearbeitung an externe Spezialisten unter Umständen sogar erforderlich machen*».

48 Les constellations discutées au sein de la doctrine reflètent encore fortement la conception selon laquelle les avocats travaillent uniquement avec des dossiers physiques renfermant des documents sous forme papier. Un traitement différencié entre processus physiques et processus numériques serait amené à s'imposer si la numérisation entraînait une restructuration fondamentale. Cela n'est cependant absolument pas le cas car, p. ex., la sauvegarde numérique d'informations confidentielles protégées par mot de passe a pour effet que les tiers ne peuvent pas prendre connaissance de ces informations même s'ils accèdent aux locaux (p. ex. les membres de l'équipe de nettoyage ou le technicien en chauffage).

49 De manière explicite, BezGer Zürich, arrêt du 18 novembre 2015, GG 150233, consid. II.2.5.4.

50 De manière explicite, BezGer Zürich, arrêt du 18 novembre 2015, GG 150233, consid. II.2.5.5, pour les travaux de rédaction effectués en Allemagne; d'un avis contraire, pour ce qui concerne les actes entrepris à l'étranger: SCHWANINGER/LATTMANN, Jusletter 11 mars 2013, N 31, étant donné que l'application du droit pénal pour les prestataires étrangers n'est pas aussi effective. À ce propos, il s'agit de préciser que les questions de juridiction pénale, voire même d'application du droit pénal, ne sont pas pertinentes pour la question de la typicité de l'infraction au sens de l'art. 321 ch. 1 premier alinéa CP (voir à ce propos plus loin, sous III.1.6). En revanche, le droit de la protection des données pose certaines limites au traitement des données à l'étranger (voir à ce propos plus loin, sous IV.3.1e)).

protégées par le secret professionnel en dehors des locaux[51]. Pour ce faire, il n'est pas nécessaire qu'ils soient engagés par le détenteur du secret, ni que l'activité soit à durée indéterminée ou rémunérée[52]. En revanche, l'auxiliaire doit soutenir directement le détenteur (principal) du secret dans son domaine d'action professionnel[53].

ii. Pas de divulgation à des auxiliaires

Le détenteur du secret ne peut pas divulguer un secret à son auxiliaire, car les auxiliaires appartiennent au cercle interne de l'organisation de travail partagé du détenteur du secret. En d'autres termes, ils deviennent partie de la même sphère de responsabilité, au sein de laquelle les participants doivent pouvoir se faire confiance mutuellement[54]. L'élément objectif de l'infraction selon l'art. 321 ch. 1

---

51 Pensons notamment à l'activité d'un détective privé, qui est compté parmi les auxiliaires (voir TF, arrêt 1B_447/2015 du 25 avril 2016, consid. 2.2.). Voir de même l'arrêt du BezGer Zürich, du 18 novembre 2015, GG 150233, consid. II.2.5.2, concernant un cas dans lequel un psychiatre avait dicté son diagnostic sur une bande sonore qu'il a ensuite envoyée à un secrétariat externe, qui a ensuite transcrit le texte dicté. Dans l'acte d'accusation, on reprochait au psychiatre d'avoir omis de requérir le consentement du patient pour la transmission du diagnostic alors qu'il était légalement tenu de le faire. Le Tribunal d'arrondissement de Zurich a considéré que les collaborateurs du secrétariat qui ont exécuté le travail de transcription étaient des auxiliaires du médecin et que ceux-ci étaient soumis à la même obligation de garder le secret que les employés de cabinets médicaux et d'hôpitaux. C'est pourquoi le médecin n'a pas violé son devoir de confidentialité en faisant usage d'une prestation de service externe. Cf. à ce propos également FISCHER, 11.

52 BezGer Zürich, arrêt du 18 novembre 2015, GG 150233, consid. II.2.5.2 et les réf. cit.; d'un avis contraire, WOHLERS, 26, renvoyant à la situation juridique qui règne en Allemagne au regard du § 203 ancienne version D-StGB, et d'avis que la question posée par une externalisation à des tiers ne peut pas être résolue via la définition de l'auxiliaire, mais tout au plus via la présence d'un motif justificatif.

53 DONATSCH/THOMMEN/WOHLERS, 590; KELLER, 107 s. et les réf. cit.

54 PK-StGB, TRECHSEL/VEST, StGB 321 N 25; voir également, à ce sujet, la réglementation de droit civil concernant la responsabilité pour les actes entrepris par l'auxiliaire, art. 101 CO; BSK-OR-I, WIEGAND, OR 101 N 4 s. Également BezGer Zürich, arrêt du 18 novembre 2015, GG 150233, consid. II.2.5.3.

premier alinéa CP ne peut a priori être donné dans le cadre du maniement d'informations confidentielles lors de la collaboration entre le détenteur (principal) du secret et l'auxiliaire[55]. En dehors de la sphère de responsabilité commune, la protection du secret face à tous les tiers non autorisés s'applique. Les auxiliaires sont ainsi soumis à la même menace de sanction que le détenteur (principal) du secret.

iii. Simultanéité de détenteurs (principaux) du secret

Dans le cadre de certaines structures organisationnelles à travail partagé – on pense ici en particulier à une équipe soignante composée de plusieurs médecins au sein d'un hôpital –, il est reconnu qu'il peut y avoir pluralité de détenteurs (principaux) du secret[56]. Ceci est le cas p. ex. lorsque des médecins spécialisés dans différents domaines et disposant d'une expérience et d'un niveau de connaissances différents sont impliqués dans le traitement d'un même patient. Dans cette constellation aussi, une divulgation au sens de l'art. 321 ch. 1 premier alinéa CP n'est pas possible[57]. Chacun des détenteurs du secret qui y participe est cependant tenu d'observer le secret professionnel. Ce type d'intégration d'autres médecins et d'autres personnes ainsi que la manière dont ils sont tenus de traiter les informations confiden-

55 Explicite: BezGer Zürich, arrêt du 18 novembre 2015, GG 150233, consid. II.2.5.3.

56 BSK-Strafrecht II, OBERHOLZER, StGB 321 N 20; WOHLERS, 19 et 26, reprend du texte allemand la notion de «*Funktionseinheit*» (unité de fonction), mais ne voit pas, ce faisant, que le droit pénal suisse définit la figure d'auxiliaire également sous l'angle de la fonctionnalité (voir sous III.1.2b)i). La seule différence entre une structure organisationnelle de travail partagé et une répartition fonctionnelle des tâches entre le détenteur (principal) du secret et l'auxiliaire est que dans le cadre de la structure organisationnelle, le maître du secret a confié dès le départ l'information confidentielle à tous les détenteurs du secret au sein de l'équipe, respectivement que cette situation découle de la constellation de droit privé. La différence est purement graduelle.

57 DONATSCH/THOMMEN/WOHLERS, 593; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 20; PK-StGB, TRECHSEL/VEST, StGB 321 N 23; plus restrictif, WOHLERS, 19, en se basant sur la littérature relative au § 203 de l'ancienne version du D-StGB avec référence au cercle des personnes destinées à la prise de connaissance («*Kreis der zum Wissen Berufenen*»).

tielles du patient devrait idéalement être prévu déjà dans le contrat thérapeutique, à défaut de quoi on partira du principe que le patient y consent tacitement[58]. Ces considérants valent *mutatis mutandis* aussi pour une équipe d'avocates et avocats amenés à résoudre conjointement un cas juridique complexe.

iv. Position WOHLERS concernant l'auxiliaire

Dans son avis de droit rédigé sur mandat du préposé à la protection des données du canton de Zurich, WOLFGANG WOHLERS soutient sur deux points essentiels des points de vue divergents qui se basent surtout sur des sources issues de l'ancien droit allemand (§ 203 de l'ancienne version du D-StGB)[59].

---

[58] KELLER, 114 ss.

[59] Malheureusement, l'avis de droit ne distingue pas toujours entre la littérature suisse et les essais d'interprétation développés autour de l'art. 321 CP, d'une part, ni les textes allemands pris en compte sur le plan du droit comparé, d'autre part. Ainsi, WOHLERS se base plusieurs fois sur des sources qui se réfèrent au § 203 de l'ancienne version du D-StGB. Le § 203 de l'ancienne version du D-StGB présentait certes des similitudes avec l'art. 321 CP, mais également des différences notables. Ainsi, la condition de la plainte manque au § 203 de l'ancienne version du D-StGB, la norme inclut à son al. 2 également les fonctionnaires et, en particulier, le rôle des «*Hilfspersonen*» du droit pénal allemand était défini différemment («*berufsmässig tätige Gehilfen*», cf. § 203 al. 3 seconde phrase de l'ancienne version du D-StGB). Selon la doctrine dominante, en Allemagne, un tiers externe qui exécutait de manière indépendante des mandats pour le détenteur d'un secret au sens du § 203 al. 1 n'était pas considéré comme un auxiliaire, ce qui découlerait «*zwar nicht schon zwingend aus dem Begriff des Gehilfen, wohl aber aus dem Grundgedanken der Vorschrift*»; cf. p. ex. LENCKNER, in: Schönke/Schröder, 27e éd. D-StGB 203 N 64 et les réf. cit. (ancienne version). La conception terminologique dans le cadre du processus législatif en Suisse et en Allemagne était également différente (en particulier concernant la notion d'auxiliaire, cf. sous III.1.2b)i). En raison de l'interprétation restrictive du § 203 de l'ancienne version du D-StGB, la disposition a entretemps dû être révisée afin de mieux satisfaire à l'aspect du travail partagé dans le domaine d'activités du détenteur du secret. La version actuelle est entrée en vigueur le 09.11.2017 avec la nouvelle la loi allemande du 30.10.2017 régissant la protection du secret en cas de participation de tiers à l'exercice de la profession de personnes tenues au secret professionnel (Gesetz zur Neuregelung des

D'une part, WOHLERS conteste le fait que le résultat constaté ci-avant (ii) selon lequel un détenteur (principal) du secret ne peut pas révéler un secret à un auxiliaire et que de ce fait la typicité de l'infraction tombe déjà: «*Hinzuweisen ist (…) an dieser Stelle darauf, dass die Einbeziehung der Hilfspersonen in den Kreis der Schweigepflichtigen nicht bedeutet, dass die Weitergabe des Geheimnisses an sie per se als straflos anzusehen ist. Ein derartiger Schluss liesse sich mit dem allgemein anerkannten Grundsatz nicht vereinbaren, dass auch die Weitergabe an Schweigepflichtige den Straftatbestand erfüllen kann*»[60]. La note de bas de page relative à cette phrase renvoie à un autre passage du texte, où figure ce qui suit: «*Auch die Weitergabe an einen anderen Amts- und Berufs- geheimnisträger kann ein Offenbaren darstellen*». Ici, on est en présence d'une conclusion erronée du fait d'un amalgame entre deux constellations de départ différentes. Lorsqu'une avocate ou un avocat, ou encore un médecin ou un procureur, qui sont tous tenus, selon les art. 320 et 321 CP, de garder un secret de fonction ou professionnel porté à leur connaissance, fait part d'une information qui tombe sous le secret professionnel, il est clair que l'on a à faire ici à une révélation au sens de l'art. 321 ch. 1 premier alinéa CP, à moins qu'une obligation légale ou le consentement du maître du secret justifie cette révélation (constella-

Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen, BGBl. I p. 3618). Une comparaison avec le droit pénal autrichien aurait au demeurant montré que dans ce pays comme en Suisse, la notion de «*Hilfskräfte*» (auxiliaires) y est définie plus largement et sous l'angle fonctionnel; cf. concernant le secret professionnel en Autriche § 121 Ö-StGB, qui n'est cependant pas applicable aux avocats: Wiener Kommentar, LEWISCH, Ö-StGB 121 N 15, et les réf. cit.

60 WOHLERS, 21 s. Encore plus clairement WOHLERS, 25 s.: «*Tatsächlich kann* (…) *aus der Existenz der Kategorie der Hilfspersonen als taugliche Täter nicht gefolgert werden, dass auch die Weitergabe an sie für den primären Geheimnisträger straflos sein soll. Die Kategorisierung als Hilfsperson ändert deshalb für sich gesehen nichts daran, dass die Weitergabe der Daten als Offenbarung eines Geheimnisses einzustufen ist*» (c'est nous qui le soulignons). WOHLERS, digma 2017, 114 s., où cette constellation n'est plus évoquée.

tion 1)[61]. Malgré le devoir du médecin ou du procureur de garder le secret de fonction ou professionnel, ils sont considérés comme des tiers non autorisés par rapport à l'avocat. La manière dont le détenteur (principal) du secret est autorisé à communiquer avec son auxiliaire est cependant une toute autre question à laquelle il faut répondre indépendamment de cette constellation. Dans cette seconde constellation, une transmission du secret ne peut jamais être une divulgation. En effet, si l'on considère la collaboration sous l'angle fonctionnel, le fait que les auxiliaires entrent en contact avec le secret, respectivement en prennent connaissance via le détenteur (principal) du secret, soit du fait qu'ils effectuent des recherches sur le cas ou en dactylographient, traitent ou archivent des éléments, soit du fait qu'ils procèdent régulièrement à la maintenance du système informatique du détenteur (principal) du secret, entreprennent des mises à jour du système informatique en faisant usage de droits d'administrateur ou fournissent d'autres services de support, alors que les données confidentielles restent disponibles pendant l'exécution de ces tâches (constellation 2), constitue justement un élément de la définition. Les passages d'argumentation mentionnés par WOHLERS ne permettent pas non plus de soutenir sa position[62]. ATF 114 IV 44, consid. 3.b, BezGer Uster, arrêt du 20 mars 1996[63], BERGER[64], DONATSCH/THOMMEN/WOHLERS [65], ISENRING[66], KELLER[67], PIETH[68], RASEL-

[61] Avis divergent de l'OGer Aargau, arrêt du 15 décembre 1983, RSJ 81/1985, 146 s., selon lequel la transmission à un détenteur du secret professionnel externe n'est pas constitutif de l'infraction si celui-ci est lui aussi soumis au secret professionnel (entre médecins).

[62] WOHLERS, 17 s., n. 65.

[63] BezGer Uster, arrêt du 20 mars 1996, ZR 96/1997, 266 ss. Dans cet arrêt, les auxiliaires sont en outre considérés explicitement et sans exception comme faisant partie du cercle des détenteurs du secret (p. 266).

[64] BERGER, recht 2000, 187.

[65] DONATSCH/THOMMEN/WOHLERS, 593 et les réf. cit.

[66] ISENRING, StGB/JStGB-Kommentar, StGB 320 N 15, StGB 321 N 10.

[67] KELLER, 114 s. et les réf. cit.

[68] PIETH, 131.

LI[69], STRATENWERTH/BOMMER[70] et STRATENWERTH/WOHLERS[71] se réfèrent incontestablement et exclusivement à la constellation 1. En outre, également STRATENWERTH/WOHLERS[72] retiennent explicitement qu'une révélation à des auxiliaires n'est pas constitutive d'une infraction, ce qui rejoint les résultats de notre analyse.

Au final, on constate qu'il n'existe aucune constellation dans laquelle une transmission de l'information à un auxiliaire ou une prise de connaissance par un auxiliaire constituerait une révélation au sens de l'art. 321 ch. 1 premier alinéa CP.

Ensuite, WOHLERS défend une conception extrêmement restrictive de la question de savoir qui peut être considéré comme un ou une auxiliaire. Notre analyse a montré qu'en droit pénal suisse, l'auxiliaire est compris de manière large et fonctionnelle[73]. WOHLERS, en revanche, défend une interprétation étroite en s'appuyant sur des sources relatives au § 203 de l'ancienne version du D-StGB. Il s'appuie en particulier sur une figure juridique jusqu'alors inhabituelle dans la doctrine suisse, à savoir le «*Kreis der zum Wissen Berufenen*». Il exprime par là le fait que le maître du secret désigne une personne ou un cercle de personnes avec qui il souhaite partager le secret[74]. Au regard de l'orientation clairement fonctionnelle de la définition de l'auxiliaire de l'art. 321 ch. 1 premier alinéa CP, cette figure juridique est trompeuse. Le législateur suisse entendait expressément ne pas réduire le cercle des personnes pouvant être amenées à prendre connaissance du se-

69 RASELLI, ZStR 1993, 32 s. et les réf. cit.

70 STRATENWERTH/BOMMER, § 61 N 7.

71 STRATENWERTH/WOHLERS, StGB 320 N 3, StGB 321 N 4.

72 STRATENWERTH/WOHLERS, StGB 320 N 3, StGB 321 N 4.

73 Cf. sous III.1.2b)i), avec de nombreuses références.

74 WOHLERS, 16, 18 et 26; les arguments se rapportent tous au § 203 de l'ancienne version du D-StGB. De même, WOHLERS, 20, lorsqu'un bénéficiaire de services externalisés a accès aux données et clés cryptographiques utilisées, parce qu'il n'appartiendrait pas au cercle des personnes appelées à connaître du secret («*nicht zum Kreis der zum Wissen Berufenen*»). De même, WOHLERS, digma 2017, 116.

cret aux personnes appelées à connaître du secret («*zum Wissen Berufenen*»), mais a au contraire inclus, dès le début, les personnes qui entrent en contact avec les informations confidentielles dans le cadre de leur collaboration avec le détenteur (principal) du secret parce qu'elles rédigent, copient ou archivent des documents, ou parce qu'elles fournissent des prestations qui peuvent entraîner une prise de connaissance d'informations confidentielles. De ce fait, il n'est pas soutenable d'affirmer que l'art. 321 CP part «*von einem System des Informationsmanagements aus, (…) das darin besteht, dass Informationen bestimmten individuellen Geheimnisträgern anvertraut und grundsätzlich von diesem* mit niemandem *geteilt werden*»[75].

v. Choix et surveillance de l'auxiliaire

Aussi dans le cas d'une définition fonctionnelle large de l'auxiliaire en droit pénal suisse, se pose la question de savoir si le choix de l'auxiliaire demeure du seul pouvoir d'appréciation du détenteur du secret, ou si des règles doivent être observées en la matière[76]. Le droit civil ainsi que les règles de déontologie peuvent apporter des réponses. Les règles de déontologie ne peuvent certes pas autoriser une révélation interdite par le droit pénal[77], mais éventuellement contribuer à concrétiser la notion d'auxiliaire de l'art. 321 ch. 1 premier alinéa CP dans le cadre d'une interprétation téléologique.

Pour les avocates et avocats, l'obligation de discrétion découle pour l'essentiel de leur obligation de ne pas porter atteinte à la personnalité du client (art. 28 CC), de leur responsabilité obligationnelle pour une

---

75 WOHLERS, 14, mise en évidence dans l'original; de même, WOHLERS, digma 2017, 114.

76 WOHLERS, 16; WOHLERS, digma 2017, 115, qui est, sur la base de son interprétation restrictive, de l'avis que le contrôle du cercle des personnes autorisées à prendre connaissance des informations confidentielles ne saurait être confié à l'avocate ou l'avocat.

77 NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 16; voir également: BSK-OR I, WEBER, OR 398 N 11.

bonne et fidèle exécution du mandat (art. 398 al. 2 CO) ainsi que de l'art. 12 let. a LLCA en lien avec l'art. 13 LLCA[78] . En faisant appel à un ou une auxiliaire, l'avocate ou l'avocat ne viole pas son obligation de diligence basée sur le droit civil et sur l'obligation de surveillance[79]. Selon le message du Conseil fédéral du 28 avril 1999 sur la LLCA, la notion d'auxiliaire au sens de l'art. 13 al. 2 LLCA correspond à celle d'auxiliaire au sens de l'art. 101 CO[80]. Ainsi, l'auxiliaire est une personne tierce à laquelle l'avocate ou l'avocat confie certaines tâches[81].

En impliquant un ou une auxiliaire, l'avocate ou l'avocat ne profite pas seulement des avantages qu'offre le partage des tâches mais devient en même temps responsable des éventuels désavantages qui pourraient en découler pour le client[82]. Ainsi, ils endossent la responsabilité au sens de l'art. 101 CO pour tous les dommages causés par l'auxiliaire dans le cadre de l'exécution de ses obligations, dans la mesure où l'on pourrait en principe les leur reprocher. La question de savoir si une libération contractuelle de la responsabilité est compatible avec l'art. 101 al. 3 CO et la LLCA est contestée[83], mais pas décisive en la matière. En effet, l'art. 13 al. 2 LLCA exige des avocates et avocats qu'ils veillent, de par leurs choix, surveillance et instructions des auxiliaires, à ce que le secret professionnel soit respecté[84]. Si une avocate ou un avocat n'entreprend pas tout ce que l'on peut raisonnablement exiger d'elle ou de lui afin que l'auxiliaire conserve le se-

78 En détail: CR-LLCA, MAURER/GROSS, LLCA 13 N 11 ss; SCHILLER, N 383 ss.

79 BSK-OR I, WEBER, OR 398 N 3; NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 50.

80 FF 1999 6013, 6056.

81 BOHNET/MARTENET, § 11 N 1861; CHAPPUIS, 178 ss; FELLMANN, N 555 et 634; CR-LLCA, MAURER/GROSS, LLCA 13 N 93; NATER/ZINDEL in: Fellmann/Zindel, BGFA 13 N 51.

82 ATF 114 Ib 67, consid. 2.c; BSK-OR I, WIEGAND, OR 101 N 2.

83 Voir REHMANN, RSJ 2017, 134; SCHILLER, N 1627 ss; FELLMANN, in: Fellmann/Zindel, BGFA 12 N 27a.

84 SCHILLER, N 540 ss; voir aussi: CHAPPUIS/ALBERINI, Revue de l'avocat 2017, 341.

cret professionnel, elle ou il viole alors cette règle de droit[85]. La doctrine exige que les auxiliaires soient soumis à l'obligation contractuelle de garder le secret[86], tout en soulignant que, selon la taille et le domaine d'activités du cabinet d'avocats, un dispositif de sécurité peut être nécessaire dans les faits[87]. Une activité professionnelle exercée avec soin exige par suite que les informations soient partagées selon le principe du «*need-to-know*»[88]. Ainsi, en cas d'informations particulièrement sensibles, il peut se révéler nécessaire de réduire le cercle des auxiliaires impliqués[89].

Il apparaît donc clairement que le détenteur du secret n'est pas entièrement libre de choisir l'auxiliaire selon son bon vouloir. Cependant, le législateur a reconnu la nécessité de faire participer des auxiliaires et a laissé la définition du cercle d'auxiliaires à la libre interprétation. La question d'une désignation à chaque fois explicite de l'auxiliaire par le maître du secret n'a pas été discutée lors de l'édiction de la norme, et ce processus n'est pas non plus exigé par la loi[90]. C'est

---

85 SCHILLER, N 540; NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 56 s.

86 CR-LLCA, MAURER/GROSS, LLCA 13 N 101; SCHILLER, N 541; NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 56; voir également: DSB ZÜRICH, Tätigkeitsbericht 2017, 18.

87 NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 56 s. On pensera p. ex. à la gestion des clés cryptographiques, qui reste de la responsabilité du cabinet d'avocats dans le modèle de services IaaS (cf. II.3.2) ou au contrôle d'accès dans le cadre des modèles de services IaaS et SaaS (II.3.3), qui reste toujours de la responsabilité du cabinet d'avocats (cf. également IV.3.1d)).

88 NATER/ZINDEL, in: Fellmann/Zindel, BGFA 13 N 43.

89 Ainsi, notamment, en cas de reprise d'entreprises cotées en bourse ou pour les personnalités publiques, des murailles dites de Chine («*chinese walls*») sont mises en place; voir, concernant l'organisation d'un «*data room*» dans le cadre d'une due diligence: ROSENTHAL, in: Rosenthal/Jöhri, OR 328b N 57. Selon les cas, les auxiliaires impliqués dans la recherche juridique ne sont pas informés de l'identité du mandataire. Pour les banques, la mise en place de murailles de Chine en cas de reprise représente même une règle de conduite sur le marché dans le cadre du droit de surveillance (cf. TSCHÄNI/DIEM, 129, en particulier N 351).

90 Ainsi, à ce jour, il est absolument inhabituel de demander une autorisation de confier au personnel du secrétariat des tâches au sein d'une étude d'avocats.

pourquoi il est nécessaire de rechercher la solution dans les limites de la loi, en examinant le sens et le but de la norme. Ce faisant, le principe directeur peut être formulé comme suit: toutes les tâches qui sont objectivement nécessaires et usuelles dans le contexte professionnel de la gestion des processus administratifs dans le cadre d'une répartition judicieuse du travail au sein d'un cabinet médical ou d'avocats ou pour toute autre activité du détenteur du secret peuvent être déléguées par le détenteur (principal) du secret à des auxiliaires, et ce, sans autorisation spécifique du maître du secret[91]. Pour le choix de l'auxiliaire, les prescriptions civiles et déontologiques qui s'appliquent complémentairement en vertu de l'interprétation téléologique et qui permettent de procéder à une délimitation judicieuse doivent être observées. Le secret ne perd aucunement sa protection du fait de l'implication d'auxiliaires car, comme déjà évoqué[92], les auxiliaires risquent les mêmes sanctions pénales s'ils violent l'obligation de conserver le secret.

Si l'avocate ou l'avocat n'est pas, d'une manière générale, libre de décider avec qui elle ou il partage les informations confidentielles,

---

91 D'un avis contraire, WOHLERS, 19, en se référant à la notion de «*Kreis der zum Wissen Berufenen*», quoique ALTHAUS STÄMPFLI, 143 (relativement à l'art. 47 LB), cité pour soutenir la prise de position, tend plutôt à la position ici défendue: «*Grundsätzlich ist davon auszugehen, dass der durchschnittliche Kunde darauf vertraut, dass die Informationen und Daten, welche er seinem Kundenbetreuer anvertraut, nur denjenigen Personen weitergegeben werden, welche einen Beitrag an die vom Kunden beanspruchten Dienstleistungen leisten. Dies steht nicht im Widerspruch zum Interesse des Kunden und damit zum Grundsatz ‹Kenntnis nur soweit nötig›*». De même pour ce qui concerne le mandant d'une avocate ou d'un avocat ou le patient d'un médecin, il faut partir du principe que le maître du secret présuppose une répartition du travail utile et usuelle au sein du cabinet médical ou d'avocats. ALTHAUS STÄMPFLI, 143 (concernant l'art. 47 LB): «*Jeder Kunde weiss, dass eine Bank oder ein Finanzintermediär heute als arbeitsteilige Organisation ihre Dienstleistungen durch verschiedene Abteilungen erbringt*». Toujours est-il, selon WOHLERS, 21, qu'un accord (présomptif) doit pouvoir être admis «*wo die Offenbarung zur sachgerechten Erledigung der vom Geheimnisherrn gewünschten Dienstleistung unabdingbar* [*ist*]», avec renvoi à KELLER, 108.

92 Voir à ce propos ci-avant, au point III.1.2b)i.

cela vaut aussi pour le choix du fournisseur de services de cloud en tant qu'auxiliaire[93]. Comme pour les autres auxiliaires, l'avocate ou l'avocat doit aussi engager contractuellement le fournisseur de services de cloud à observer le secret professionnel. En pratique, il lui faudra examiner les CG du fournisseur de services de cloud en conséquence. En outre, selon la LLCA, l'avocate ou l'avocat est tenu de surveiller, dans une mesure que l'on peut raisonnablement exiger d'elle ou de lui, que l'obligation de garder le secret est observée.

Certains revendiquent que les avocates et avocats soient tenus de pourvoir à un enregistrement des données en Suisse ou de choisir un prestataire suisse en arguant du fait qu'à défaut, des autorités étrangères non liées par le secret professionnel pourraient accéder aux données[94]. D'abord, pour ce faire, il ne peut s'agir que du siège du fournisseur de services de cloud ou du lieu de travail effectif du technicien, car l'emplacement du serveur ne revêt pas la qualité de sujet de droit contre lequel de telles décisions pourraient être exécutées. D'un point de vue dogmatique, cette distinction ne peut cependant pas non plus être justifiée, étant donné que l'implication d'auxiliaires étrangers est en principe admise par l'art. 321 CP et que lors de processus communicationnels, on ne peut souvent éviter de faire appel à des auxiliaires étrangers. Une étude d'avocats qui communique avec des parties adverses, tribunaux, témoins ou experts étrangers ne peut éviter de transmettre des informations protégées par le secret professionnel à des fournisseurs de services d'e-mails, des bureaux de poste auxiliaires ou des prestataires de services de télécommunications étrangers. L'avocate ou l'avocat doit décider, en tenant compte des aspects pertinents en matière de secret professionnel et du niveau de sensibilité des informations, si l'implication des auxiliaires étrangers en question est justifiable au vu du risque encouru. Il n'existe pas

93 WOHLERS, digma 2017, 115, semble en revanche partir du principe que le choix de l'auxiliaire est laissé au gré de l'avocate ou de l'avocat.

94 CHAPUIS/ALBERINI, Revue de l'avocat 2017, 341; similairement: SCHWANINGER/LATTMANN, Jusletter 11 mars 2013, N 31.

d'obligation générale de choisir un fournisseur de services de cloud suisse sur la base de l'art. 321 CP[95]. Lors de l'évaluation de l'adéquation du risque, il s'agit surtout de prendre en considération la sensibilité des données, mais également le respect envers le contrat et la loi que l'on peut attendre du fournisseur de services de cloud étranger ainsi que la probabilité d'un accès aux données. Cette évaluation des risques peut varier en fonction de l'activité des avocats; il convient d'être particulièrement prudent notamment lorsque l'on conseille des clients étrangers sur des questions fiscales et des clients politiquement exposés[96].

vi. Conclusion provisoire

Pour ce qui concerne la notion d'auxiliaire, on peut retenir que l'interprétation large et fonctionnelle défendue ici est affirmée par le sens littéral de l'art. 321 CP, le contexte systématique, les sources législatives historiques ainsi que les considérations téléologiques. Cette interprétation est en outre représentée par la doctrine dominante[97]. La conception étroite de WOHLERS, qui se base surtout sur l'ancien droit allemand, ne convainc pas.

Ainsi, il est certain que pour les activités à travail partagé au sein d'études d'avocats, toutes les personnes qui soutiennent le détenteur

95 Selon le type d'activités du cabinet d'avocats, une telle obligation pourrait découler de l'interdiction du service de renseignement économique au sens de l'art. 273 CP, selon lequel personne n'est autorisé à rendre accessible à un destinataire étranger un secret d'affaire ou de fabrication suisse (dans ce sens: WAGNER/ZWIRNER, 174 n. 42 ; avec des réserves : VLCEK, 176). Cette disposition doit cependant être interprétée de manière restrictive (ROSENTHAL, in: Rosenthal/Jhöri, StGB 273 N 64), respectivement, on réclame que le Conseil fédéral ne puisse conférer que de manière restrictive les pouvoirs nécessaires pour la poursuite pénale (art. 66 LOAP), pour des actes commis à l'étranger (BSK- Strafrecht II, HUSMANN, StGB 273 N 79).

96 Voir, à ce sujet également, l'analyse sur l'externalisation du traitement de données vers les USA, sous l'angle de la protection des données, sous IV.3.1f).

97 Voir à ce sujet III.1.2b)i.

(principal) du secret d'une manière telle qu'elles puissent avoir connaissance d'informations confidentielles doivent être qualifiées d'auxiliaires. Aucune autorisation explicite par le maître du secret n'est nécessaire. Sont comptés parmi les auxiliaires les responsables de l'informatique au sein des cabinets d'avocats, tout comme les entreprises de services informatiques externes qui assurent le traitement, l'enregistrement et l'archivage des informations des études d'avocats, assurent la maintenance du système d'exploitation et prennent des mesures de sécurité. Les auxiliaires ne doivent pas être liés par des relations de travail avec le détenteur (principal) du secret et ils peuvent aussi accomplir leurs tâches d'auxiliaire en dehors des locaux administratifs du détenteur (principal) du secret. Les activités d'auxiliaire à l'étranger ne sont pas exclues. Les fournisseurs de solutions de cloud (IaaS, SaaS) font également partie du cercle des auxiliaires.

La protection du secret ne devient en aucun cas caduque en raison de l'implication d'auxiliaires, ni en général, ni en particulier du fait de l'utilisation de services de fournisseurs de services de cloud[98], parce que l'obligation de confidentialité et les menaces de sanction valent aussi pour tous les auxiliaires. En outre, le droit de la protection des données pose des limites au traitement externe des données par un tiers, et le détenteur (principal) du secret est tenu responsable pour les auxiliaires en vertu de l'art. 101 CO.

c) Acte délictueux: divulgation

Les éléments constitutifs objectifs de la révélation sont donnés si le détenteur du secret porte ce dernier à la connaissance d'un tiers non autorisé[99] ou permet à ce tiers d'en prendre connaissance. Peu im-

[98] Voir cependant WOHLERS, 10.

[99] PK-StGB, TRECHSEL/VEST, StGB 321 N 23 «(*mindestens*) *ein Aussenstehender*»; les auxiliaires sont des personnes autorisées. Le secret ne peut pas leur être révélé de manière à satisfaire à la typicité de l'infraction (cf. ci-avant III.1.2b)ii); d'un avis contraire, WOHLERS, 26.

porte de quelle manière cela a lieu. Les types d'actes délictueux suivants sont au premier plan[100]: la communication orale ou écrite, la remise de documents écrits ou d'autres éléments qui révèlent le secret, l'envoi de données électroniques (texte, image, son, vidéo) ainsi que la mise à disposition de données électroniques sur un support de données accessible à au moins un tiers non autorisé. Cependant, l'acte peut aussi être commis par omission improprement dite[101], p. ex. par une conservation déficiente des documents[102].

Ci-dessus, nous avons déjà évoqué le flou dogmatique autour du fait que pour parler de consommation de l'infraction selon la doctrine dominante, la prise de connaissance par au moins un tiers non autorisé est présupposée, ce qui ne peut être donné dans le cas d'une simple mise à disposition ou de l'oubli d'un dossier dans un bureau[103]. Même si le destinataire est déjà en possession de l'information confidentielle suite à des rumeurs ou la conjecture, un secret peut être considéré révélé du moment où la divulgation aboutit à un savoir fiable et sûr[104].

Pour les informations ou données anonymisées ou cryptées dont le contenu ne peut être parlant, il n'y a pas de divulgation, même si des

---

100 ATF 75 IV 71, consid. 1; ATF 112 Ib 606, consid. b; DONATSCH/THOMMEN/WOHLERS, 593 et les réf. cit.; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 19; STRATENWERTH/BOMMER, § 61 N 19; WOHLERS, 17; WOHLERS, digma 2017, 115; comp. FELLMANN, N 560.

101 BSK-Strafrecht II, OBERHOLZER, StGB 321 N 19; PK-StGB, STRATENWERTH/BOMMER, § 61 N 7 et 19; STRAUB, PJA 2010, 552 et 555; TRECHSEL/VEST, StGB 321 N 23.

102 Concernant les exigences posées pour l'archivage des dossiers, les prescriptions de droit de la protection des données découlant des art. 7 LPD et 8 OLPD peuvent être invoquées, étant donné que les dossiers sont régulièrement des collectes de données au sens de la LPD et renferment souvent des données sensibles au sens de l'art. 3 let. c LPD. Les avocats sont libérés de l'obligation de déclarer de l'art. 11a LPD; cf. BSK-DSG/BGÖ, BLECHTA, DSG 11a N 14d. Concernant la conservation: BSK-DSG/BGÖ, BLECHTA, DSG 7 N 7.

103 Voir ci-avant sous III.1.1.

104 ATF IV 71, consid. 1; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 19.

personnes extérieures peuvent prendre connaissance des donnée elles-mêmes[105]. L'archivage de données cryptées dans le nuage informatique (IaaS) ne remplit donc déjà pas les éléments objectifs de l'infraction de l'art. 321 CP. Pour les modèles SaaS (voir le scénario 2 sous II.3.3), le fournisseur de services de cloud dispose, du point de vue technique, de l'accès aux données enregistrées dans le document. Dans une telle constellation, une divulgation est possible.

Selon l'interprétation présentée ci-avant, les personnes en charge des services informatiques de l'avocate ou de l'avocat ou qui exploitent pour elle ou lui des services de nuage informatique sont – même s'il s'agit de prestataires externes – des auxiliaires au sens de l'art. 321 ch. 1 premier alinéa CP. Les informations concernant les mandants peuvent leur être rendues accessibles sans qu'il s'agisse d'une divulgation[106]. Autrement dit: la typicité de l'infraction tombe en cas de transmission ou de mise à disposition de données entre le détenteur (principal) du secret et ses auxiliaires.

1.3 Éléments subjectifs de l'infraction

D'un point de vue subjectif, un acte commis intentionnellement est nécessaire, le dol éventuel étant suffisant. Donc, si l'auteur du délit est conscient du fait qu'il pourrait divulguer un secret et qu'il accepte cette éventualité, les éléments constitutifs de l'infraction sont donnés (art. 12 al. 2 CP)[107].

---

105 BERGER, recht 2000, 191 et les réf. cit.; BLATTMANN, in: Baeriswyl/Rudin, IDG 6 N 13; PK-StGB, TRECHSEL/VEST, StGB 321 N 23; WOHLERS, 20; EDÖB, 14. Tätigkeitsbericht, 51.

106 D'un avis contraire, WOHLERS, 20, qui ne considère pas le sous-traitant comme un auxiliaire. Cet auteur est d'avis qu'il y a divulgation dès le moment où le sous-traitant est en mesure de déchiffrer les informations confidentielles. Le même principe s'applique d'après lui pour la maintenance des logiciels.

107 PK-StGB, TRECHSEL/VEST, StGB 321 N 26; STRATENWERTH/BOMMER, § 61 N 20; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 21.

Les éléments subjectifs de l'infraction sont pertinents lorsqu'un auxiliaire divulgue un secret à un tiers non autorisé. Se pose ensuite la question de savoir si le détenteur (principal) du secret est également punissable pour violation du secret professionnel. On devrait répondre à cette question par l'affirmative si le détenteur (principal) du secret sait d'emblée ou, du moins, juge possible que l'auxiliaire révélera l'information confidentielle, et qu'il accepte ce résultat. Mais en règle générale, cela n'est pas le cas et seul l'auxiliaire sera ainsi punissable pénalement. Le détenteur (principal) du secret peut cependant être poursuivi le cas échéant au civil, en application de l'art. 101 CO.

1.4 Illicéité

Selon l'art. 321 ch. 2 CP, la révélation ne sera pas punissable si elle a été faite avec le consentement de l'intéressé ou si, sur la proposition du détenteur du secret, l'autorité supérieure ou l'autorité de surveillance l'a autorisée par écrit. Le chiffre 3 quant à lui réserve les dispositions de la législation fédérale et cantonale relatives à l'obligation de témoigner en justice et à l'obligation de renseigner une autorité.

Notre analyse a montré que les responsables de l'informatique au sein d'un cabinet d'avocats ainsi que les fournisseurs externes de solutions de cloud doivent être considérés comme des auxiliaires au sens de l'art. 321 ch. 1 premier alinéa CP. Ces auxiliaires peuvent exercer leur activité pour le détenteur du secret sans autorisation expresse du maître du secret[108]. Pour cette raison, nous nous bornerons à nous pencher dans ce paragraphe sur les conditions et les effets d'une autorisation accordée par le maître du secret dans le contexte de l'externalisation de services informatiques dans un nuage informatique, dans le seul sens d'une protection complémentaire (à caractère justificatif)[109]. Dans le sens d'une telle protection complémentaire, il

[108] Voir ci-avant, sous III.1.2b).

[109] Pour BLATTMANN, in: Baeriswyl/Rudin, IDG 6 N 10, l'autorisation a pour but de se prémunir contre une décision judiciaire négative («*nicht dem Risiko eines nega-*

peut être judicieux de demander au maître du secret, dans le cadre du contrat de mandat, une autorisation préalable de recourir à un prestataire de services de cloud, mais également, de manière générale, à des auxiliaires mis régulièrement à contribution (p. ex. des suppléants ou des responsables de l'informatique). Une telle procédure permet une transparence face au client et a un effet justificatif[110] en droit pénal et de protection des données[111].

Dans la mesure où une autorisation permet l'entière révélation de l'information confidentielle, le comportement ne peut plus être délictueux, puisqu'aucun tort ni aucune violation de la sphère privée du maître du secret ne peut être commis. Si en revanche la révélation de l'information confidentielle n'est autorisée qu'à certaines personnes ou certains services, le consentement revêt alors le caractère d'un motif justificatif[112]. Dans le cadre de l'activité d'avocat, il s'agit en général de ce dernier cas de figure. Les principes généraux relatifs à l'autorisation à caractère justificatif s'appliquent[113].

a) Consentement du titulaire du droit

La condition préalable est le pouvoir de disposition sur le bien juridique, à savoir qu'il doit s'agir d'un bien juridique individuel. Cette condition préalable est remplie[114]. Le maître du secret peut limiter son

tiven richterlichen Urteils auszusetzen»). D'autres motifs de justification ne se présentent que dans des cas d'exception: cf. WOHLERS, 26 s.

110 Voir à ce sujet sous IV.3.1b) et IV.3.2a); WOHLERS, 26, parvient à la conclusion, sur la base de son interprétation plus restrictive, que l'externalisation de tâches auxiliaires à des tiers externes ne peut exclure la punissabilité que si un motif justificatif se présente, en particulier en cas d'autorisation.

111 Voir à ce sujet sous IV.

112 OGer Zürich, décision du 30 août 2016, SB160142, consid. 3.4.1.b; DONATSCH/THOMMEN/WOHLERS, 599; BSK- Strafrecht II, OBERHOLZER, StGB 321 N 22; STRATENWERTH/BOMMER, § 61 N 22; PK-StGB, TRECHSEL/VEST, StGB 321 N 28.

113 De manière générale, au sujet de l'autorisation: SEELMANN/GETH, 50; PK-StGB, TRECHSEL/GETH, StGB 14 N 11 et les réf. cit.

114 Art. 321 ch. 2 CP; voir sous III.1.1. La personne autorisée correspond à la personne lésée légitimée à déposer une demande en justice, ATF 75 IV 75 consid. 3; PK-

autorisation à une personne, un objet, un destinataire ou encore quant au moment de la communication[115].

b) Capacité de consentir

La capacité de discernement est requise pour que le consentement déploie des effets juridiques. Au moment de consentir, le maître du secret doit saisir correctement les circonstances concrètes et être en mesure d'agir avec discernement. La loi propose une définition négative de la capacité de discernement, à savoir qu'en principe, elle est présupposée (cf. art. 16 CC)[116]. La capacité de discernement étant relative en raison du fait qu'elle dépend du contexte social et de la complexité de l'état de fait à juger, les personnes incapables d'agir peuvent, selon les circonstances, également être considérées comme capables de discernement. En cas d'incapacité de discernement, la décision incombe au représentant légal, bien entendu dans les limites du devoir de protection[117]. Pour les patients incapables de discernement, l'intérêt au maintien du secret est présupposé[118].

StGB, TRECHSEL/VEST, StGB 321 N 28. Seul le maître du secret peut donner son autorisation, mais la personne concernée par le secret n'est pas forcément la même que celle qui l'a confié: BLASS, RSJ 1966, 337; CR-CP II, CHAPPUIS, CP 321 N 140; DUPUIS ET AL., CP 321 N 38, 40; KELLER, 137; REHBERG, Bulletin des médecins suisses 1969, 235; STRATENWERTH/BOMMER, § 61 N 22; PK-StGB, TRECHSEL/VEST, StGB 321 N 28.

115 DE HALLER, Schweizerische Versicherungs-Zeitschrift, 1980, 9; DUPUIS ET AL., CP 321 N 42; KELLER, 146; PK-StGB, TRECHSEL/VEST, StGB 321 N 28.

116 BSK ZGB I, BIGLER-EGGENBERGER/FANKHAUSER, ZGB 16 N 2 et les réf. cit.

117 P. ex., une représentation pour les questions relevant de la sphère privée n'est pas admise. BSK ZGB I, BIGLER-EGGENBERGER/FANKHAUSER, ZGB 16 N 5 ; CR-CP II, CHAPPUIS CP 321 N 141; CORBOZ, SJ 1993, 91 ss; DONATSCH/THOMMEN/WOHLERS, 599; DUPUIS ET AL., CP 21 N 40; KELLER, 140; SEELMANN/GETH, 52; STRATENWERTH, § 10 N 21; PK-StGB, TRECHSEL/VEST, StGB 321 N 28.

118 PK-StGB, TRECHSEL/VEST, StGB 321 N 28.

c) Absence de vice du consentement et «*informed consent*»

Le consentement du maître du secret doit être le fait de sa libre volonté. Ce faisant, le maître du secret doit exprimer son consentement en pleine connaissance du genre et de la portée de la divulgation du secret et de toutes les circonstances essentielles. En outre, la formation de sa volonté ne doit pas être altérée par la contrainte, la menace ou la tromperie[119].

Afin que les conditions soient remplies, le maître du secret doit être suffisamment informé de la manière dont les dossiers, données et informations sont traités («*informed consent*»)[120]. En conséquence, le maître du secret doit être éclairé sur l'objet, le but et l'étendue de la transmission des données prévue. Ces éléments peuvent être spécifiés dans le cadre d'une procuration ou d'un contrat de mandat.

Selon WOHLERS, une déclaration de consentement peut en principe aussi avoir lieu par formulaire, comme p. ex. par la signature, au début de la relation client, du formulaire d'inscription contenant la précision correspondante. En revanche, l'obtention d'une autorisation globale non spécifique via un formulaire ou des conditions générales ne remplirait pas, selon lui, les conditions d'un consentement valable[121]. Ainsi, la question de savoir s'il est possible de donner son autorisation au moment du début d'une relation de mandat est sujette à caution, au vu de la condition du caractère déterminé du secret à divulguer. WOHLERS procède à une comparaison avec le patient qui signe un formulaire de déliement du secret médical du médecin face à son assurance, même s'il ne peut pas encore connaître, à ce moment-

119 BOHNET/MARTENET, § 11 N 1905; KELLER, 141 ss; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 22; SEELMANN/GETH, 53; STRATENWERTH, § 10 N 22; WOHLERS, 29; WOLFFERS, 39.

120 OGer Zürich, décision du 30 août 2016, SB160142, consid. 3.4.1.b, en citant l'exemple d'une transmission de données du patient à des tiers; KELLER, 142; PIETH, 131.

121 WOHLERS, 28.

là, la portée de son autorisation. Cette comparaison est cependant bancale du fait que dans le cadre de la relation de mandat entre le client et son avocate ou avocat, les informations confidentielles sont déjà suffisamment déterminables, et que le client est tout à fait en mesure de prendre une décision «informée» sur la base de la présentation de la manière dont seront traitées ses données[122].

d) Forme et moment du consentement

En application des principes généraux, l'autorisation doit être donnée avant l'exécution de l'acte délictueux[123]. L'opinion selon laquelle une autorisation pourrait déployer un effet justificatif également après la divulgation du secret ne nous paraît pas défendable[124]. Après consommation de l'acte, le maître du secret ne dispose «que» de la possibilité de renoncer à déposer une plainte pénale (et de celle de la retirer). Dans la mesure où un cabinet d'avocats recourt déjà à des prestations de fournisseurs de services de cloud, il est cependant imaginable, pour les relations de mandats en cours, de demander après coup encore une autorisation du client relative à l'utilisation de ces services. Ce consentement doit alors être compris dans le sens d'une autorisation pour une utilisation future. Si l'utilisation a déjà eu lieu, l'autorisation correspond à une déclaration de désintéressement ou, dans la mesure où les prescriptions de forme sont observées (art. 302 al. 2 CPP), à une renonciation au sens de l'art. 30 al. 5 CP[125].

---

122 BERGER, recht 2000, 193; SCHÄFER, 55; STOCKER, 249.

123 BOHNET/MARTENET, § 11 N 1908; CORBOZ, SJ 1993, 93; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 22; SEELMANN/GETH, 50.

124 CR-CP II, CHAPPUIS, CP 321 N 146; CORBOZ, SJ 1993, 93; DUPUIS ET AL., CP 321 N 44.

125 BSK-Strafrecht I, RIEDO, StGB 30 N 119 ss et les réf. cit. Cette déclaration de désintéressement peut également être prononcée à l'égard de tiers, et en particulier à l'égard de l'auteur du délit.

La loi ne prescrit pas de forme particulière pour l'autorisation de l'ayant droit[126]; une déclaration de volonté unilatérale peut cependant être exprimée soit de manière expresse, soit par actes concluants[127].

En cas d'autorisation par actes concluants, la volonté du maître du secret de renoncer à la préservation du secret doit être clairement exprimée. Cependant, selon le Tribunal fédéral, il suffit p. ex. déjà, pour la libération du secret professionnel, que l'ayant droit appelle le détenteur du secret à témoigner dans le cadre d'un procès[128]. Dans le domaine médical, on part du principe que l'autorisation vaut également pour l'implication nécessaire d'autres médecins spécialistes, dans la mesure où rien d'autre ne découle du mandat de traitement. De même, dans le cadre des relations entre le médecin prescripteur et le médecin traitant ainsi que dans le cadre de la poursuite du traitement et du traitement complémentaire, l'échange d'informations se fait dans l'intérêt du patient[129]. Selon DONATSCH/THOMMEN/WOHLERS, le seul fait que la transmission des informations puisse se faire dans l'intérêt du patient ou du client ne saurait justifier de présumer une autorisation par actes concluants. La volonté de renoncer à la préser-vation du secret doit plutôt être exprimée clairement[130]. Selon KELLER, l'expérience générale de la vie commande de partir du principe d'une autorisation en cas d'actes concluants[131]. On peut p. ex. présumer une autorisation tacite du patient pour la divulgation des faits aux autres médecins d'un conseil de médecins lorsque ceux-ci sont conjointement en charge

126 Cependant, une autorisation expresse par écrit est à recommander.

127 ATF 97 II 369, 370; 98 IV 217, consid. 2; BezGer Uster, ZR 96/1997, 295; CR-CP II, CHAPPUIS CP 321 N 144; DE HALLER, Schweizerische Versicherungs-Zeitschrift 1980, 19; DONATSCH/THOMMEN/WOHLERS, 599; DUPUIS ET AL., CP 321 N 41; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 22; STRATENWERTH/BOMMER, § 61 N 22; PK-StGB, TRECHSEL/VEST, StGB 321 N 28; UTTINGER/LIEBRENZ, Bulletin des médecins suisses 2014, 1745.

128 ATF 97 II 369, 370; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 22.

129 KELLER, 114 ss; BSK-Strafrecht II, OBERHOLZER, StGB 321 N 20; PK-StGB, TRECHSEL/VEST, StGB 321 N 28.

130 DONATSCH/THOMMEN/WOHLERS, 599; BezGer Uster, ZR 96/1997, 289-303.

131 KELLER, 144.

du traitement du patient. Ainsi, en cas de prise en charge médicale conjointe par plusieurs médecins, chacun d'entre eux ne devra pas procéder à nouveau à l'anamnèse et entreprendre lui-même tous les examens[132]. Le même principe doit être retenu pour le traitement d'un mandat par plusieurs avocates et avocats et pour l'implication d'un fournisseur de services de cloud.

Si une avocate ou un avocat demande à son client l'autorisation de communiquer des informations confidentielles dans le but de se prémunir complémentairement, le client peut accorder cette autorisation sans être lié par des conditions de forme. En revanche, on ne pourra partir du principe d'un accord tacite que si le comportement du client exprime clairement son consentement à la divulgation d'informations confidentielles au fournisseur de services de cloud. Ceci est déjà donné lorsque l'avocate ou l'avocat attire l'attention de son client sur l'implication d'un fournisseur de services de cloud pour l'enregistrement et le traitement des données qui concernent le mandat et que le client poursuit sans hésiter la relation de mandat. Une autorisation expresse serait encore plus explicite.

e) Agissement en connaissance du consentement

En application des règles générales du droit, une autorisation ne peut avoir un effet justificatif que si l'«auteur» a eu connaissance de l'autorisation avant d'agir[133]. S'il agit sans ce savoir, il se trouve alors dans l'erreur, ce qui a un effet désavantageux pour lui, dans le sens que son comportement serait alors considéré comme une tentative de commettre un délit.

Si une autorisation est accordée dans le cadre d'une procuration ou d'un contrat de mandat qui renferment les modalités exhaustives du

---

132 KELLER, 115; REHBERG, Bulletin des médecins suisses 1969, 235; SCHÄFER, 29; TIMM, 33.

133 KELLER, 139; SEELMANN/GETH, 53; STRATENWERTH, § 10 N 24.

traitement des dossiers, données et informations du client, ce critère ne pose alors pas de problème en l'espèce.

f) Révocabilité du consentement

Découlant de la liberté d'action générale, l'autorisation est, en sa qualité de déclaration de volonté unilatérale sujette à réception et formatrice de droit, révocable à tout moment. Cependant, la révocation ne peut déployer des effets que pour le futur[134].

1.5 Plainte pénale

Une poursuite pénale présuppose que le maître du secret dépose une plainte pénale. Au sens de l'art. 321 CP, est habilité à déposer une plainte pénale non seulement le client, mais également tout maître du secret, soit toute personne concernée directement pas la révélation du secret, indépendamment du fait que cette personne soit un client de l'avocate ou de l'avocat ou non[135].

1.6 États de fait internationaux

a) Droit de la peine applicable et typicité de l'infraction

Le droit de la peine applicable détermine le moment auquel une norme de droit pénal suisse peut être applicable dans l'espace[136]. La question de savoir si l'application du droit pénal suisse est une condition de recevabilité, une règle d'attribution *sui generis* ou une condi-

134 CR-CP II, CHAPPUIS, CP 321 N 146; KELLER, 143 s.; SEELMANN/GETH, 50; SIEBEN, 88.

135 NIGGLI, Revue de l'avocat 2006, 279; RIEDO, 217 s.; PK-StGB, TRECHSEL/VEST, StGB 321 N 27.

136 SCHWARZENEGGER, RPS 2000, 114; GLESS, N 119. Selon la jurisprudence du TF, il s'agit d'admettre la compétence de la Suisse également dans les cas ne présentant pas de lien étroit avec notre pays, afin d'éviter des conflits de compétence négatifs (ATF 141 IV 205, consid. 5.2).

tion objective de punissabilité est controversée[137]. Il est en revanche incontesté que la question de la validité du droit pénal suisse prime l'attribution pénale au sens étroit[138]. La question de savoir si un comportement litigieux est soumis à la juridiction pénale suisse doit ainsi être examinée en priorité et indépendamment de la question de savoir si celui-ci constitue un état de fait régi par le droit pénal suisse.

b) Application du droit pénal en cas de délit de lésion et de résultat

Étant donné que le délit commis en violation de l'art. 321 CP présuppose à la fois une lésion et un résultat[139], deux principaux éléments de rattachement sont donnés en application de l'art. 3 al. 1 CP en lien avec l'art. 8 CP (principe de la territorialité et principe de l'ubiquité relatif) pour déterminer la juridiction pénale en Suisse, soit le lieu où l'auteur a agi et celui où le résultat s'est produit[140]. L'élément de rattachement principal dans le droit de la peine applicable est le lieu de commission de l'acte[141]. Pour les délits dont les actes d'exécution consistent en la communication vers l'extérieur, la propagation, la présentation ou la mise à disposition (transmission des données ou délits de communication), le lieu auquel se trouve l'auteur du délit au moment de l'acte de divulgation physique ou numérique est déterminant. Dans le contexte des réseaux, il s'agit de la saisie de l'ordre de transmission ou de sauvegarde destiné à transférer vers le disque dur d'un ordinateur (serveur web, serveur e-mail, serveur du nuage informatique) des données qui peuvent alors être consultées par au

137 GLESS, N 120 ss et les réf. cit.

138 GLESS, N 120; EICKER, § 3 N 3.

139 Voir ci-avant, sous III.1.1.

140 En cas d'omission, le lieu de commission est celui où l'auteur du délit aurait dû agir. En cas de tentative, le lieu où l'auteur a perpétré l'acte ainsi que le lieu auquel il s'attendait à ce que le résultat se produise sont tous deux considérés comme lieux de commission de l'acte (art. 8 al. 2 CP).

141 DYENS, 159 ss; MUGGLI, 187 ss; BSK-Strafrecht I, POPP/KESHELAVA, StGB 8 N 1 s.; SCHWARZENEGGER, RPS 2000, 117 ss, et les réf. cit. respectives. Cf. également l'art. 31 CPP concernant la primauté du lieu de commission.

moins un tiers non autorisé[142]. Si cet acte a lieu en Suisse, la violation du secret professionnel peut ainsi être poursuivie en Suisse. Si, en revanche, un fournisseur de services de cloud agissant en tant qu'auxiliaire est situé à l'étranger au moment de l'acte de divulgation, le délit correspondant est considéré commis à l'étranger. Dans de tels cas, un rattachement n'est possible qu'au lieu du résultat[143]. Le résultat selon l'art. 321 CP constitue en la prise de connaissance par un tiers quelconque non autorisé. Le lieu du résultat au sens de l'art. 8 al. 1 CP est ainsi le lieu auquel cette prise de connaissance a lieu. Si, au moment de la prise de connaissance, le tiers non autorisé se trouve à l'étranger, un rattachement selon le principe de la territorialité n'est pas possible (art. 3 CP en lien avec l'art. 8 CP). Le critère de rattachement du résultat comprend une part de hasard, le lieu où se trouve le tiers non autorisé au moment de la prise de connaissance pouvant être n'importe quel endroit[144]. La juridiction pénale selon le principe de la territorialité est ainsi en principe donnée pour un avocat suisse détenteur (principal) du secret[145], de sorte que la poursuite pénale à l'intérieur du pays ne semble pas problématique. Néanmoins, étant donné que l'intention du détenteur (principal) du secret pourra rarement être prouvée[146], la punissabilité reste exclue pour des raisons matérielles.

Alternativement, la juridiction pénale suisse se fonde sur le principe passif de la personnalité (art. 7 CP)[147]. Si un maître du secret suisse est concerné, un délit commis à l'étranger peut être poursuivi en Suisse si

142 BSK-Strafrecht I, POPP/KESHELAVA, StGB 8 N 4 ss; SCHWARZENEGGER, RPS 2000, 118 s. et les réf. cit.

143 Concernant le lieu du résultat, cf. BSK-Strafrecht I, POPP/KESHELAVA, StGB 8 N 9 ss; SCHWARZENEGGER, RPS 2000, 119 ss et les réf. cit.

144 Critique sur ce point, BSK-Strafrecht I, POPP/KESHELAVA, StGB 8 N 10 s.

145 Une telle juridiction devrait exceptionnellement être niée si l'avocate ou l'avocat se trouve à l'étranger au moment de la divulgation du secret.

146 Voir ci-avant, sous III.1.3.

147 Concernant le principe passif de la personnalité, à titre complémentaire, BSK-Strafrecht I, POPP/KESHELAVA, StGB avant 3 N 21; StGB 7 N 1 ss et les réf. cit.

la violation du secret professionnel est également réprimée au lieu de commission à l'étranger, si l'auteur du délit se trouve en Suisse ou s'il est extradé vers à la Suisse en raison de cet acte et si, selon le droit suisse, l'acte peut donner lieu à l'extradition[148], mais que l'auteur n'est pas extradé vers le pays où il a commis l'acte (comp. art. 7 al. 1 CP)[149]. L'obstacle majeur à la poursuite pénale en Suisse de tels délits commis à l'étranger constitue dans le fait que l'auteur du délit qui agit à l'étranger ne se rendra sans doute pas volontairement en Suisse, ou que l'extradition par le pays étranger n'a pas lieu car ce pays n'extrade pas ses propres citoyens, ou encore que le lieu de commission du délit ne peut pas être déterminé.

Nous retiendrons en conclusion que les violations du secret professionnel perpétrées à l'étranger ne tombent pas toutes sous la juridiction pénale suisse. Dans les cas décrits, soit lorsque l'acte punissable ou le résultat n'ont pas lieu en Suisse, la protection du secret par les autorités de poursuite pénale suisses semble de fait limitée. Une poursuite en application du principe passif de la personnalité dépend de plusieurs conditions préalables limitatives. D'autre part, il s'agit de préciser qu'une violation du secret professionnel est également punissable dans la plupart des pays étrangers, et que le maître du secret dispose de la possibilité de déposer en tout temps une plainte pénale auprès des autorités de poursuite pénale étrangères. En outre, les autorités de poursuite pénale suisses peuvent en tout temps déposer une demande de compétence pénale déléguée[150].

148 La condition d'une peine maximale d'une durée minimum d'un an de peine privative de liberté est remplie pour la violation évoquée à l'art. 321 CP; voir l'art. 35 al. 1 EIMP.

149 D'autres limitations se présentent lorsque le maître du secret n'est pas suisse; cf. art. 7 al. 2 CP.

150 Art. 88 s. EIMP.

2. Violation de l'obligation de garder le secret professionnel

2.1 Éléments objectifs de l'infraction

a) Cercle des auteurs de l'infraction et objet de l'atteinte

L'art. 35 LPD sanctionne la révélation non autorisée de données personnelles secrètes, et sensibles, ainsi que la révélation de profils de la personnalité. Étant donné que le secret doit être donné de manière cumulative afin que les données qu'il contient soient qualifiées de sensibles, l'objet de l'infraction y est défini plus étroitement qu'à l'art. 321 CP[151]. Au sens de l'art. 3 let. c LPD, les données personnelles sensibles sont les données sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, les données sur la santé, la sphère intime ou l'appartenance à une race, les données sur des mesures d'aide sociale ainsi que les données sur des poursuites ou sanctions pénales et administratives. Les profils de la personnalité sont définis à l'art. 3 let. d LPD comme constituant un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique. En outre, ces données personnelles sensibles ou profils de la personnalité doivent être secrets. Les données sont secrètes lorsqu'elles sont relativement inconnues et que le maître du secret a un intérêt légitime au maintien de leur caractère secret[152].

L'art. 35 LPD définit un délit véritablement spécial. L'auteur du délit ne peut être qu'une personne qui exerce un métier qui requiert la connaissance de données personnelles secrètes et sensibles ou de profils de la personnalité, et qui a effectivement obtenu de telles données dans le cadre de l'exercice de sa profession[153]. La disposition englobe

151 ROSENTHAL, in: Rosenthal/Jhöri, DSG 35 N 1.

152 ROSENTHAL, in: Rosenthal/Jhöri, DSG 35 N 9 et les réf. cit.

153 BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 40.

ainsi uniquement certains secteurs professionnels[154]. Sont également punissables les personnes qui divulguent les données en question alors qu'elles sont des auxiliaires de la personne exerçant l'activité professionnelle en question ou qu'elles sont en formation chez elle[155]. Ce faisant, les critères d'application sont les mêmes que ceux de l'art. 321 ch. 1 premier alinéa CP[156].

b) Acte délictueux

Est sanctionnable la communication de données personnelles secrètes et sensibles. L'art. 3 let. f LPD définit la communication comme le fait de rendre des données accessibles. La loi cite à titre d'exemple la transmission et la diffusion des données ainsi que l'autorisation de les consulter[157]. Est englobé tout procédé qui permet à des tiers de prendre connaissance du contenu des données[158].

2.2 Éléments subjectifs de l'infraction

D'un point de vue subjectif, un acte commis intentionnellement est nécessaire, le dol éventuel étant suffisant. Il suffit que l'auteur du délit prenne en compte la possible divulgation des données personnelles secrètes sensibles et qu'il accepte cette éventualité (art. 12 al. 2 CP)[159].

---

154 BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 8; le législateur a cité l'exemple des assistants sociaux, des courtiers matrimoniaux et des psychologues (FF 1988 II 413, 485). Notons que depuis le 1er avril 2013, les psychologues figurent également à l'art. 321 premier alinéa CP.

155 BezGer Zürich, arrêt du 18 novembre 2015, GG 150233, consid. II.2.5.6; BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 10.

156 BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 12 et les réf. cit.

157 SHK-DSG, RUDIN, DSG 3 N 41.

158 BSK-DSG/BGÖ, BLECHTA, DSG 3 N 77; BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 15.

159 Cf. BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 42.

2.3 Plainte pénale

Selon une partie de la doctrine, le maître du secret est la personne légitimée à déposer une plainte[160], soit la personne qui a communiqué les données litigieuses au détenteur du secret, en vue de l'exercice de l'activité professionnelle. Selon l'avis contraire, est légitimée à déposer plainte la personne concernée au sens du droit de la protection des données (cf. art. 3 let. b LPD), à savoir la personne dont il est question dans les données personnelles.[161] Le maître du secret et la personne concernée ne doivent pas être identiques. C'est p. ex. le cas lorsqu'un assistant social a appris de la personne prise en charge (maître du secret) que le partenaire de cette dernière (personne concernée) fait l'objet d'une poursuite pénale. Étant donné que l'art. 35 LPD est destiné à combler une lacune dans la protection du secret professionnel[162], il semble approprié que, par analogie, le droit de plainte n'appartienne qu'au maître du secret en cas de violation du secret professionnel.

2.4 Concurrence

Les conditions posées par l'art. 321 comme celles posées par l'art. 35 LPD peuvent être remplies en cas de révélation ou de communication d'informations si l'auteur du délit réunit les deux caractéristiques particulières. La doctrine part du principe que les art. 321 CP et 35 LPD se trouvent en concours idéal improprement dit, à savoir que la violation de l'obligation de garder le secret professionnel est consommée par la violation du secret professionnel[163].

---

160 BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 67.

161 ROSENTHAL, in: Rosenthal/Jhöri, DSG 35 N 4 et DSG 34 N 22.

162 FF 1988 II 413, 485.

163 BSK-DSG/BGÖ, NIGGLI/MAEDER, DSG 35 N 74; SHK-DSG, PÄRLI, DSG 35 N 12; cf. cependant ROSENTHAL, in: Rosenthal/Jhöri, DSG 35 N 17, selon lequel l'art. 35 LPD ne s'applique que de manière «subsidiaire».

IV. Droit de la protection des données

1. Remarques préliminaires

L'utilisation de services de cloud par les avocates et avocats doit avoir lieu en accord avec les prescriptions du droit de la protection des données lorsque les fournisseurs de ces services traitent des données personnelles au sens de la loi sur la protection des données. Si l'élément du traitement de données personnelles n'est pas donné, notamment parce que les avocates et avocats cryptent les données avant de les transmettre[164], le droit de la protection des données ne s'applique pas à l'activité du fournisseur de services de cloud.

En cas de traitement de données personnelles, la question se pose de savoir quel droit s'applique. Au premier plan se trouvent le droit suisse de la protection des données (LPD) ainsi que le règlement général de l'UE sur la protection des données (RGPD). Si des données personnelles de clientes et clients étrangers sont traitées, ce traitement par le fournisseur de services de cloud peut cependant être soumis aux lois d'un autre ordre juridique lorsque les règles de droit international privé applicables en l'espèce le prévoient. Le présent avis de droit se limite cependant à examiner la question de l'évaluation sous l'angle de la LPD en vigueur, du projet de LPD révisée (P-LPD) ainsi que du RGPD.

Dans le présent avis de droit, nous nous contentons d'examiner la question de savoir selon quelles conditions préalables et dans quelles constellations l'activité des avocates et avocats suisses est soumise au RGPD. C'est pourquoi il suffit de montrer ici que le RGPD peut s'appliquer dans de nombreuses constellations et comment l'utilisation de services de cloud par les avocates et avocats suisses doit avoir lieu afin que les prescriptions du RGPD soient observées

[164] Voir à ce sujet sous II.3.2.

lorsque celles-ci viennent à s'appliquer. Les questions d'exécution et de surveillance ne seront pas non plus examinées[165].

2. Applicabilité

2.1 Droit applicable

a) Loi fédérale sur la protection des données (LPD)

Le traitement des données personnelles par des avocates et avocats en Suisse et l'utilisation de services de cloud dans ce but sont en principe soumis à la LPD. Ce, du moins dans la mesure où les faits ont lieu en Suisse, soit lorsque des avocates et avocats suisses traitent des données de clients suisses en faisant appel à des fournisseurs de services de cloud suisses. Si un état de fait présente en revanche un lien qualifié avec un pays autre que la Suisse, un droit étranger peut trouver application sur la base de la LDIP. Ceci n'est cependant pas obligatoire, car la LDIP peut aussi renvoyer à la LPD suisse. La personne concernée – p. ex. une cliente étrangère – peut notamment choisir, selon l'art. 139 al. 3 en lien avec l'al. 1 let. b LDIP, de soumettre ses prétentions issues du droit de la protection des données au droit de l'État dans lequel l'auteur de l'atteinte, soit dans ce cas l'avocate ou l'avocat suisse, a son établissement ou sa résidence habituelle.

b) Règlement général sur la protection des données (RGPD)

i. Applicabilité extraterritoriale du RGPD

Le RGPD suit le principe d'établissement et du lieu auquel se tient le marché (*lex loci solutionis*) (cf. art. 3 al. 2 RGPD). Tombent sous le coup du RGPD (i) le traitement des données dans le cadre des activités d'un établissement d'une personne responsable ou d'un mandataire au sein de l'Union européenne, (ii) l'offre de marchandises ou de

[165] Voir à ce sujet: BENHAMOU/JACOT-GUILLARMOD, digma 2018, *passim*; HOEREN, EuZ 2018, *passim*; AZZI, JIPITEC 2018, 132.

prestations à des personnes au sein de l'UE, ainsi que (iii) l'observation du comportement de personnes qui se trouvent dans l'UE.

Avec le principe du lieu auquel se tient le marché, le RGPD exerce son devoir de protection garanti par les droits fondamentaux vis-à-vis des citoyens de l'UE et entend créer un marché équitable («*level playing field*») pour le marché de l'UE[166]. L'activité d'avocates et d'avocats suisses peut tout à fait tomber sous le coup du RGPD[167], notamment lorsque leur offre s'adresse à des clients de l'UE. La notion «s'adresse à» doit, en se basant sur le considérant 23 RGPD, être interprétée à la lumière de la jurisprudence de la CJUE[168], raison pour laquelle l'accès à un site Internet depuis l'UE n'est en soi pas suffisant[169]. Les prestations doivent plutôt revêtir un caractère international, ce qui peut en particulier découler de l'utilisation d'un domaine étranger ou international de premier niveau, d'un plan d'accès pour clients étrangers ou encore d'une publicité avec des évaluations de clients issus de pays de l'UE[170].

En outre, selon le considérant 22 RGPD, un traitement de données sur mandat (voir à ce propos sous IV.3.2a)) au sein de l'UE doit remplir les conditions posées par le RGPD, peu importe que le traitement ait lieu au sein de l'UE ou non. Cependant, cela ne signifie pas que chaque recours à un traitement de données sur mandat au sein de

166 ENÖCKL, in: Sydow, DSGVO 3 N 17.

167 STEIGER, Revue de l'avocat 2018, 206.

168 Voir CJUE, arrêt du 7 décembre 2010, C-585/08 et C-144/09, Pammer/Alpenhof concernant l'interprétation de la notion d'exercice d'une activité professionnelle au regard de l'art. 15 al. 1 let. c du Règlement de Bruxelles I. Cette jurisprudence est déjà d'importance pour les entreprises suisses actives effectuant des transactions commerciales au sein de l'UE en application de l'art. 15 al. 1 CL (cf. ZERDICK, in: Ehmann/Selmayr, RGPD 3 N 19; GEORGE/TAMÒ, 39 s.; AZZI, JIPITEC 2018, 129).

169 CJUE, arrêt du 7 décembre 2010, C-585/08 et C-144/09, Pammer/Alpenhof, N 69; HOEREN, EuZ 2018, 162 s.; PRAZ, PJA 2018, 610.

170 CJUE, arrêt du 7 décembre 2010, C-585/08 et C-144/09, Pammer/Alpenhof, N 83.

l'UE conduit à l'applicabilité du RGPD pour les entreprises suisses. Le domaine d'application du RGPD découle de la teneur de l'art. 3 RGPD. Le motif d'un considérant peut expliquer ou préciser le texte du règlement, mais non imposer lui-même des obligations[171]. Les destinataires du RGPD sont en premier lieu les entreprises sises dans l'UE, et le considérant 22 précise que celles-ci restent tenues d'assurer l'observation du RGPD, même si elles externalisent un traitement des données par un tiers hors de l'UE[172].

Le RGPD fait partie du droit supranational de l'UE. Bien qu'il soit applicable directement en tant qu'ordonnance de l'UE, il ne permet pas d'assurer une harmonisation totale[173]. Il n'est pas rare que certaines activités soient interdites et que le législateur national ait la possibilité de déroger aux prescriptions du RGPD au moyen d'une clause d'ouverture[174]. Se pose par suite la question de savoir quel droit national de transposition est applicable à un état de fait transnational. Comme le RGPD ne contient pas de règles de conflit de lois, la question est déjà sans réponse pour ce qui concerne les relations entre

171 CJUE, arrêt du 13 juillet 1989, C-215/88, *Casa Fleischhandel*, N 31.

172 PRAZ, PJA 2018, 610; PILTZ, in: Gola, DSGVO 3 N 5: «*Abs. 2 regelt Konstellationen, in denen der Verantwortliche oder Auftragsverarbeiter, zumindest dem Wortlaut nach, gar nicht in der EU niedergelassen ist*». Cf. également VASELLA, digma 2017, *passim*, cependant avec un autre fondement.

173 LAUE, ZD 2016, 464.

174 STEIGER, Revue de l'avocat 2018, 205; ainsi p. ex., les informations concernant les condamnations pénales ne doivent être élaborées que sous la surveillance d'une autorité ou si le droit des États membres ou de l'UE le prévoit (art. 10 RGPD). Même si cela ne signifie pas une interdiction de traitement de telles données, mais entend seulement en garantir un maniement responsable («*verantwortungsvoll*») (SCHIFF, in: Ehmann/Selmayr, DSGVO 10 N 1), p. ex. le droit irlandais prévoit qu'il est permis de procéder au traitement de données concernant des condamnations pénales, dans le cadre de la fourniture de prestations juridiques ou pour faire valoir des droits (art. 55(1)(b) Irish Data Protection Act 2018).

les États membres[175]. Ceci vaut a fortiori pour l'application extraterritoriale du RGPD en Suisse.

La question de savoir si un cabinet d'avocats oriente ses activités vers l'UE doit être examinée au cas par cas, en particulier au regard de sa présentation sur le web. Notamment les études d'avocats d'une certaine taille orientent régulièrement leur offre (également) vers des clients de l'UE. Mais aussi les cabinets d'avocats plus petits peuvent remplir ce critère, p. ex. si leur lettre d'information attire l'attention sur des développements du droit susceptibles d'intéresser tout particulièrement des clients de l'UE. En accord avec le but poursuivi par le RGPD, seules les données qui sont traitées sur la base d'une orientation vers le marché européen tombent sous le droit européen[176]. Par suite, les dispositions du RGPD ne doivent être prises en compte que pour les données de clients européens.

ii. Applicabilité sur la base de la LDIP

Si une procédure est pendante devant un tribunal suisse, le droit applicable est déterminé par la LDIP. Lors d'une procédure devant un tribunal étranger, le droit applicable serait déterminé par le droit international privé de la *lex fori* en question. Subséquemment, seule la première constellation peut être couverte. Les questions de la compétence internationale sont également écartées.

Le droit de la protection vise à protéger la personnalité de la personne concernée (art. 1 LPD). Si une personne dont la personnalité a été violée par un traitement des données porte plainte devant les tribunaux suisses, le droit applicable est déterminé à l'aune de l'art. 139 al. 3 en lien avec l'art. 139 al. 1 LDIP: vient ainsi à s'appliquer, au choix du

175 PILTZ, in: Gola, DSGVO 3 N 3 et 38 ss; LAUE, ZD 2016, 464, avec la constatation digne d'attention selon laquelle cela a apparemment été oublié étant donné qu'à l'origine, aucune harmonisation globale n'était planifiée.

176 STEIGER, Revue de l'avocat 2018, 206; finalement, de très nombreuses questions concernant le principe du lieu auquel se tient le marché demeurent ouvertes.

lésé, (i) le droit de l'État dans lequel le lésé a sa résidence habituelle, pour autant que l'auteur du dommage ait dû s'attendre à ce que le résultat se produise dans cet État (let. a), (ii) le droit de l'État dans lequel l'auteur de l'atteinte a son établissement ou sa résidence habituelle (let. b), ou (iii) le droit de l'État dans lequel le résultat de l'atteinte se produit, pour autant que l'auteur du dommage ait dû s'attendre à ce que le résultat se produise dans cet État (let. c). Selon la doctrine, le droit du lieu de résidence de la personne lésée peut être choisi même si le résultat dommageable ne peut pas encore être démontré[177]. Le droit du lieu de résidence habituelle peut de ce fait être invoqué en particulier pour les actions en cessation, la survenance d'un dommage étant dans ce cas souvent dans un premier temps seulement crainte[178]. Le droit du lieu du résultat ne peut en revanche être choisi qu'une fois que le dommage est survenu. Le lieu du résultat est considéré comme le lieu du premier effet immédiat produit sur le bien juridique[179]. En droit de la protection des données, il s'agit du lieu auquel les données deviennent accessibles, du lieu auquel l'effet indésirable du traitement des données commence à se produire, ou encore du lieu auquel la personne concernée se trouve au moment de l'atteinte[180]. Aussi bien le droit au lieu du résultat que le droit au lieu de résidence habituelle ne peuvent être choisis que si ces points de rattachement étaient prévisibles pour l'auteur du dommage. Étant donné que la survenance du résultat au lieu de résidence habituelle

177 BSK-IPRG, DASSER, IPRG 139 N 11; PASSADELIS, N 6.30; ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 25, avec la motivation claire selon laquelle, à défaut, la possibilité d'élection selon l'art. 139 al. 1 let. a LDIP serait absorbée par la let. c de cet article, étant donné que le lieu de résidence habituelle peut être le même que le lieu du résultat.

178 Cf. ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 25.

179 ATF 125 III 103 consid. 2b; ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 20; THALMANN, sic! 2007, 339; BÜHLMANN/REINLE, digma 2017, 10.

180 ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 22.

de la personne concernée est en principe prévisible[181], la prévisibilité limite surtout l'élection du droit applicable aux lieux du résultat.

L'élection de droit peut avoir lieu au plus tôt au moment de la survenance de l'événement fondant la prétention[182]. Est contesté le fait de savoir si le choix de la personne concernée est irrévocable[183]. La doctrine rejette à juste titre un rattachement accessoire de l'élection de droit au statut contractuel, p. ex. à une relation de mandat, en raison du but de protection de la norme[184].

Ainsi, le droit au siège de l'avocate ou de l'avocat, le droit au lieu du résultat ou le droit au lieu de résidence habituelle de la personne concernée s'applique à un traitement des données personnelles dans un nuage informatique qui viole les droits de la personnalité, dans la mesure où l'avocate ou l'avocat devait compter avec une violation de la personnalité dans ce pays. Étant donné qu'en règle générale, il faut s'attendre à la survenance du résultat au lieu de résidence habituelle du client, la LDIP suisse peut entraîner l'application du RGPD pour les avocates et avocats ayant des clients au sein de l'UE. Ce risque ne peut pas être écarté au moyen d'une élection de droit, étant donné que celle-ci n'est possible qu'une fois que la violation de la personnalité a eu lieu[185].

Si le lieu de résidence habituelle du client se trouve dans un pays de l'UE, se pose alors la question de savoir dans quelle mesure une élection de droit serait suffisante. Celle-ci englobe en principe toutes les dispositions applicables à l'état de fait, selon le droit élu (art. 13 al. 1 LDIP). Le droit national comme le droit supranational en font par-

181 ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 26; BÜHLMANN/REINLE, digma 2017, 10.

182 ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 15.

183 Cf. ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 14.

184 BSK-IPRG, DASSER, IPRG 139 N 22 et N 48; ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 16; THALMANN, sic! 2007, 340.

185 ROSENTHAL, in: Rosenthal/Jhöri, IPRG 139 N 15; PASSADELIS, N 6.31.

tie[186]. Une élection de droit du client ne peut par conséquent pas se rapporter exclusivement au RGPD. S'appliqueraient aussi bien le RGPD que le droit national mettant en œuvre le RGPD au lieu de résidence habituelle du client.

2.2 Traitement de données personnelles

a) En général

Sont considérées comme des données personnelles toutes les informations qui se rapportent à une personne identifiée ou identifiable (art. 3 let. a LPD et art. 4 al. 1 RGPD). Pour distinguer entre données personnelles et données factuelles, il est ainsi décisif de savoir si une personne est identifiable.

Même si dans leur version allemande, le RGPD et la LPD emploient des termes différents («*bestimmte oder bestimmbare Person*» dans la LPD, et «*identifizierte oder identifizierbare natürliche Person*» dans le RGPD), le concept d'identifiabilité relative est le même[187]. L'identifiabilité peut certes découler de la combinaison entre une indication et des informations complémentaires, mais une simple éventualité théorique de l'identification ne suffit pas à elle seule. L'identifiabilité est cependant donnée lorsque, selon l'expérience générale de la vie, on doit compter avec le fait qu'une personne intéressée pourrait se donner la peine d'identifier la personne en question. Ce faisant, on tiendra compte de l'état actuel de la technique et des possibilités de développement technique[188]. La question dans ce cadre est de savoir s'il faut se concentrer sur la perspective du collaborateur qui traite les données en question[189], ou si les moyens à disposition du

186 BSK-IPRG, MÄCHLER-ERNE/WOLF-METTIER, IPRG 13 N 7.

187 SCHREIBER, in: Plath, DSGVO 4 N 9 ss; BSK-DSG/BGÖ, BLECHTA, DSG 3 N 10; SHK-DSG, RUDIN, DSG 3 N 12; SPINDLER/SCHMECHEL, JIPITEC 2016, 169.

188 ATF 136 II 508, consid. 3.2; TF, arrêt 4A_365/2017 du 26 février 2018, consid. 5; CJUE, arrêt du 19 octobre 2016, C-582/14, Breyer, N 46 s.; RGPD, considérant 26.

189 SCHREIBER, in: Plath, DSGVO 4 N 9 ss.

tiers sont décisifs[190]. Si l'on suivait cette dernière conception, les critères de l'intérêt et des efforts perdraient cependant leur signification car on ne saurait pas dans quelles limites les évaluer. C'est pourquoi on se place en principe du point de vue du collaborateur qui traite les données en question. Toujours est-il que les intérêts, informations complémentaires et possibilités d'information d'un tiers doivent exceptionnellement être pris en compte si ceux-ci étaient connus ou auraient dû être connus du collaborateur qui transmet les données[191], ou si le collaborateur qui transmet les données peut accéder indirectement aux moyens évoqués[192]. Un collaborateur qui transmet des données est de ce fait lui-même soumis au droit de la protection des données lorsqu'il ne peut pas identifier lui-même une personne sur la base des données, mais qu'il transmet les données à un collaborateur qui dispose de cette possibilité tout en étant intéressé à procéder à une identification[193].

Étant donné que le lien avec la personne est relatif, il faut examiner séparément pour chaque personne impliquée si, de son point de vue, on se trouve en présence de données personnelles. Ainsi, il est tout à fait imaginable que les données en question doivent être qualifiées de données personnelles pour les avocates et avocats, mais pas pour les fournisseurs de services de cloud. Cela est notamment le cas lorsque le cryptage a lieu avant la transmission des données (voir ci-avant sous II.3.2) et que les fournisseurs de services de cloud fournissent leurs prestations sans avoir accès aux données des clients[194]. Mais ceci n'est en principe le cas que si le service reste limité au seul stockage

190 KLABUNDE, in: Ehmann/Selmayr, DSGVO 4 N 13; BSK-DSG/BGÖ, BLECHTA, DSG 3 N 11.

191 PROBST, PJA 2013, 1435; similairement: ROSENTHAL, in: Rosenthal/Jhöri, DSG 3 N 26 ss.

192 Cf. également CJUE, arrêt du 19 octobre 2016, C-582/14, Breyer, N 46 s.

193 ATF 136 III 508 consid. 3.4.

194 STRAUB, PJA 2014, 913; STAIGER, 203; RÜPKE/VON LEWINSKI/ECKHARDT, 142. Concernant la situation comparable en droit pénal: WOHLERS, digma 2017, 115.

des données[195] (voir ci-avant sous II.2.3). Il en va autrement en cas d'utilisation d'un modèle de services SaaS, dans le cadre duquel le fournisseur de services de cloud ne peut exécuter les applications logicielles que sur les données enregistrées en texte clair, soit non cryptées (voir ci-avant sous II.3.3). Dans cette constellation, le fournisseur de services de cloud a accès aux données des clients.

b) Catégories particulières de données

Les avocates et avocats peuvent enregistrer et traiter différentes catégories de données sur les serveurs des fournisseurs de services de cloud. Pour les données personnelles sensibles et les catégories particulières de données personnelles[196], des règles spéciales s'appliquent. Ceci vaut pour les données concernant la race ou l'ethnie, les idéologies et les opinions politiques, les activités syndicales ainsi que la santé et la sphère intime. Dans l'UE, ceci vaut également pour les données génétiques et biométriques, et en Suisse aussi pour les données concernant les mesures d'aide sociale, les poursuites et les peines administratives ou pénales. Il en va autrement pour les données qui concernent une poursuite pénale dans l'UE, qu'il n'est possible de traiter, selon le RGPD, que sous le contrôle de l'autorité publique (art. 10 RGPD)[197].

Selon la LPD, le traitement de données personnelles sensibles peut être justifié par la loi, le consentement ou un intérêt prépondérant (art. 13 al. 1 LPD). Si le traitement se base sur une autorisation, celle-ci

---

195 STRAUB, PJA 2014, 913.

196 La LPD emploie le terme «données sensibles» (art. 3 let. c LPD), tandis que le RGPD parle de «catégories particulières» (art. 9 RGPD). La protection spéciale de ces données est cependant déjà prescrite – du moins en partie – par la convention no 108 (art. 6 convention no 108).

197 L'énumération exhaustive est largement aléatoire et les tentatives d'élaborer des critères convaincants et d'acceptation générale pour ce qui concerne les données particulièrement sensibles n'ont pas abouti à ce jour (voir à ce sujet, déjà: SIMITIS, Festschrift Pedrazzini, 475; SHK-RUDIN, DSG 3 N 21, qui qualifie le choix d'aléatoire, de suranné et d'incomplet («*willkürlich, antiquiert und unvollständig*»).

doit être explicite (art. 4 al. 5 LPD)[198]. S'il se base sur une pesée des intérêts, la sensibilité des données doit être prise en compte lors de cette pesée des intérêts[199]. Il n'est en outre pas permis de divulguer des données personnelles sensibles en l'absence de motifs justificatifs (art. 12 al. 2 let. c LPD)[200].

Selon le RGPD, les données personnelles appartenant aux catégories particulières n'ont en principe pas le droit d'être traitées, à moins d'un état de fait spécial et exceptionnel. Pour les avocates et avocats se trouve au premier plan l'admissibilité en raison d'un consentement (art. 9 al. 2 let. a RGPD) ainsi que l'exigibilité du traitement en relation avec la constatation, l'exercice ou la défense de droits (art. 9 al. 2 let. f RGPD). La doctrine dominante rejette un traitement sur la base d'intérêts prépondérants ou d'autres états de fait selon l'art. 6 RGPD, parce que l'art. 9 RGPD doit être considéré au titre de *lex specialis* par rapport à l'art. 6 RGPD[201]. Il existe cependant des raisons convaincantes d'admettre un traitement de données également lorsqu'elles appartiennent à une catégorie particulière, sur la base d'une pesée des intérêts[202]. Pour les données relatives aux condamnations pénales et

198 SHK-DSG, BAERISWYL, DSG 4 N 71; ROSENTHAL, in: Rosenthal/Jhöri, DSG 4 N 83.

199 BSK-DSG/BGÖ, RAMPINI, DSG 13 N 23; ROSENTHAL, Datenschutz im IT-Outsourcing, 197.

200 ROSENTHAL, in: Rosenthal/Jhöri, DSG 12 N 44 s.; critique: SHK-DSG, WERMELINGER, DSG 12 N 8.

201 Explicite, au moins: SCHULZ, in: Gola, DSGVO 9 N 5; KAMPERT, in: Sydow, DSGVO 9 N 63. Voir également LAUE/NINK/KREMER, § 2 N 60; SCHIFF, in: Ehmann/Selmayr, DSGVO 9 N 10 s.

202 ROBRAHN/BREMERT, ZD 2018, 295; voir également SCHULZ, in: Gola, DSGVO 9 N 5 s., selon lequel uniquement un traitement sur la base de l'art. 6 al. 1 let. f RGPD est exclu, les autres états de fait justificatifs pouvant en revanche être invoqués. Une des raisons d'interpréter largement l'art. 9 RGPD peut être vue dans le fait que la signification symbolique de l'art. 9 RGPD est souvent opposée aux critiques (comp. SCHIFF, in: Ehmann/Selmayr, DSGVO 9 N 1 ss). En effet, si l'art. 9 RGPD est une disposition à caractère symbolique, une interprétation littérale stricte ne semble pas adéquate.

aux infractions selon l'art. 10 RGPD, cela correspond même à la doctrine dominante[203].

2.3 Conclusion provisoire

Les dispositions de la LPD ou du RGPD peuvent s'appliquer à l'utilisation de services de cloud par les avocates et avocats suisses, selon leur orientation et leur clientèle. C'est pourquoi l'évaluation en termes de droit de la protection des données suivante doit tenir compte des directives des deux réglementations. Dans la mesure où les avocates et avocats traitent des données personnelles de catégories particulières, les exigences plus strictes de la LPD et du RGPD doivent être appliquées.

La LPD et le RGPD ne s'appliquent cependant à l'utilisation de services de cloud par les avocates et avocats suisses que si les données destinées au fournisseur de services de cloud doivent être qualifiées de données personnelles. Cela n'est pas le cas si les données sont suffisamment cryptées avant leur transmission au fournisseur de services de cloud et si celui-ci ne dispose pas de la clé cryptographique. Cela ne vaut pas si le fournisseur de services de cloud, en particulier

[203] Ainsi, l'art. 10 RGPD ne prononce pas une interdiction de traitement, mais entend uniquement assurer un traitement des données qui soit responsable («*verantwortungsvoll*») lorsqu'elles ont trait à des condamnations pénales (SCHIFF, in: Ehmann/Selmayr, DSGVO 10 N 1; comp. KAMPERT, in: Sydow, DSGVO 10 N 5; GOLA, in: Gola, DSGVO 10 N 6 s.).

dans le cadre du modèle de services SaaS, exploite les logiciels pour le cabinet d'avocats dans une machine virtuelle et a ainsi – ou peut avoir ainsi – accès aux données enregistrées en texte clair dans le document (voir ci-avant sous II.3.3). Seule cette seconde constellation est pertinente sous l'angle du droit de la protection des données, et doit être examinée ci-après.

3. Traitement de données sur mandat

3.1 Selon la LPD

Le traitement de données personnelles peut être transféré à un tiers par convention ou en application de la loi. C'est le cas lors de l'utilisation de services de cloud par des avocates et avocats. Un tel traitement de données sur mandat est admis si seuls les traitements que le mandant serait en droit d'effectuer lui-même sont effectués (art. 10a al. 1 let. a LPD) et si aucune obligation légale ou contractuelle de garder le secret ne l'interdit (art. 10a al. 1 let. b LPD)[204]. Le mandant doit en particulier s'assurer que le tiers garantit la sécurité des données (art. 10a al. 2 LPD).

a) Transfert par convention

Le traitement de données personnelles par le fournisseur de services de cloud repose sur une convention entre les avocates et avocats – respectivement leur cabinet d'avocats – et le fournisseur de services. Le contrat de cloud est un contrat innommé à caractère d'obligation permanente lequel, selon la nature des services fournis (IaaS, PaaS, SaaS; voir ci-avant sous II.2), peut comporter des éléments de droit du bail, du mandat ou du contrat d'entreprise. En raison de la diversité

[204] WIDMER, digma 2014, 28; ROSENTHAL, in: Rosenthal/Jhöri, DSG 10a N 43; BSK-DSG/BGÖ, BÜHLER/RAMPINI, DSG 10a N 3; SHK-DSG, BAERISWYL, DSG 10a N 18; WAGNER/ZWIRNER, 170 s.

des formes possibles, la qualification du contrat doit être entreprise au cas par cas[205].

Les obligations principales dans le cadre d'un contrat de cloud sont la mise à disposition contre rémunération des services informatiques convenus via un réseau. D'autres aspects qui sont réglés selon la pratique sont le type d'utilisation, la collaboration avec le fournisseur de services de cloud via l'interface utilisateur, les questions de licence, les restrictions d'utilisation, la sécurité des données, la protection des données ainsi que la durée et la fin du contrat[206].

b) Traitement équivalent à celui du mandant

Les fournisseurs de services de cloud ont le droit d'effectuer seulement les traitements des données personnelles transmises par les avocates et avocats que ces derniers seraient en droit d'effectuer eux-mêmes (art. 10a let. a LPD). Ce faisant, ils peuvent invoquer les mêmes motifs justificatifs que les avocates et avocats en leur qualité de mandants (art. 10a al. 3 LPD).

Les avocates et avocats traitent régulièrement des données personnelles relatives à leurs clients, partenaires contractuels ou parties adverses ainsi que relatives à des tiers. Le traitement de ces données est admis lorsqu'il ne porte pas une atteinte illicite à la personnalité des personnes concernées (art. 12 al. 1 LPD), soit en règle générale lorsque les principes du traitement des données sont observés (art. 12 al. 2 let. a LPD), que les données ne sont pas traitées contre la volonté expresse de la personne concernée (art. 12 al. 2 let. b LPD) et qu'aucune communication de données sensibles ou de profils de la personnalité n'a lieu (art. 12 al. 2 let. c LPD). Dans le cas contraire, le traitement des données personnelles n'est admissible qu'en présence d'un motif jus-

[205] DE LA CRUZ, Jusletter IT 15 mai 2013, N 12 et 15; STRAUB, PJA 2014, 906.
[206] Voir: GRAMIGNA, Cloud-Vertrag, *passim*.

tificatif[207]. Un tel motif justificatif est donné en cas de consentement de la victime, d'un intérêt privé ou public prépondérant, ou encore en cas de base légale correspondante (art. 13 al. 1 LPD).

Les avocates et avocats traitent régulièrement des données de leurs clients sur la base de leur consentement. Cependant, ils se voient aussi souvent obligés de se fonder sur des intérêts privés prépondérants, notamment lorsqu'il s'agit de données de tiers, soit en particulier de la partie adverse. La protection des données ne s'applique pas aux procédures judiciaires pendantes (cf. art. 2 al. 2 let. c LPD) et ce, afin de ne pas éluder les règles spéciales de procédure[208].

Dans la mesure où le traitement de données personnelles par les avocates et avocats est autorisé, les fournisseurs de services de cloud ont également le droit de les traiter. Un traitement par le fournisseur dans un but propre ne serait cependant pas admissible[209]. Afin de garantir que le fournisseur de services de cloud ne traite pas les données différemment des avocates et avocats, le genre de traitement des données devrait être fixé par le fournisseur de services de cloud dans le contrat de cloud ou dans une annexe à ce contrat[210]. On pourra p. ex. y stipuler que les données ne peuvent être traitées que dans un but d'exécution du contrat, sous réserve d'instructions particulières[211].

c) Pas d'obligation opposée de garder le secret

Le traitement de données personnelles par des tiers n'est pas admissible si une obligation légale ou contractuelle l'interdit (art. 10*a* al. 1 let. b LPD). Ces obligations de confidentialité priment la réglementa-

---

207 ROSENTHAL, in: Rosenthal/Jhöri, DSG 12 N 1 s.; SHK-DSG, WERMELINGER, DSG 12 N 3.

208 Comp. JHÖRI/ROSENTHAL, in: Rosenthal/Jhöri, DSG 2 N 29; SHK-RUDIN, DSG 2 N 26.

209 SHK-DSG, BAERISWYL, DSG 10a N 26.

210 ROSENTHAL, in: Rosenthal/Jhöri, DSG 10a N 71.

211 ROSENTHAL, in: Rosenthal/Jhöri, DSG 10a N 72.

tion sur le traitement des données sur mandat[212]. Cependant, le traitement des données sur mandat n'est pas interdit d'emblée en raison de l'obligation de garder le secret, mais uniquement si les prescriptions légales ou contractuelles ne sont pas observées[213]. La recevabilité du traitement de données sur mandat en cas d'obligation de garder le secret dépend de l'admissibilité de la révélation selon les dispositions applicables en matière d'obligation de garder le secret[214]. Comme nous l'avons présenté ci-avant[215], l'utilisation de services de cloud par les avocates et avocats ne viole pas les obligations légales de garder le secret. L'utilisation de services de cloud peut en revanche violer d'éventuelles obligations contractuelles de garder le secret.

d) Obligations de garantie et de surveillance, en particulier sécurité des données

Dans le cadre du traitement de données sur mandat, le mandant reste responsable du respect des dispositions du droit de la protection des données[216]. L'art. 10a LPD stipule clairement que le mandant doit s'assurer que le mandataire effectue seulement les traitements de données qu'il serait en droit d'effectuer lui-même[217]. En outre, la sécurité des données doit en particulier être garantie (art. 10a al. 2 LPD). Comme le mandant reste juridiquement responsable de l'observation du droit de la protection des données alors que le fournisseur de services de cloud est techniquement responsable, en particulier dans le cadre des modèles de services SaaS (voir ci-avant sous II.3), d'autres

212 FF 1988 II 464; ROSENTHAL, in: Rosenthal/Jhöri, DSG 10a N 101; SHK-DSG, BAERISWYL, DSG 10a N 29.

213 SHK-DSG, BAERISWYL, DSG 10a N 29; du même avis: WOHLERS, digma 2016, 115.

214 BSK-DSG/BGÖ, BÜHLER/RAMPINI, DSG 10a N 13; SHK-DSG, BAERISWYL, DSG 10a N 35 s.; du même avis: WOHLERS, digma 2016, 115.

215 Voir ci-avant sous III.

216 GRAMIGNA, Cloud-Vertrag, N 30; SHK-DSG, BAERISWYL, DSG 10a N 2; BSK-DSG/BGÖ, BÜHLER/RAMPINI, DSG 10a N 11; SURY/GOGNIAT, Revue de l'avocat 2015, 204.

217 ROSENTHAL, in: Rosenthal/Jhöri, DSG 10a N 46; BSK-DSG/BGÖ, BÜHLER/RAMPINI, DSG 10a N 11.

éléments doivent être réglés lors de l'attribution du mandat[218]. Par analogie avec l'art. 55 CO, les trois *curae* s'appliquent au mandant, soit celles *in eligendo*, *in instruendo* et *in custodiendo*[219]. Cependant, ni la LPD ni l'OLPD ne règlent la manière dont le mandant doit remplir ces obligations.

Celui ou celle qui traite des données personnelles doit les protéger contre des traitements entrepris par des tiers non autorisés, en prenant des mesures techniques et organisationnelles appropriées (art. 7 LPD). L'OLPD concrétise cet objectif à son art. 8 al. 1 de manière à ce que celui ou celle qui traite les données soit responsable de leur confidentialité, de leur disponibilité et de leur intégrité. Ce faisant, il lui faut garantir que les données personnelles sont traitées à l'interne de manière conforme à la loi et qu'il n'est pas non plus possible à des tiers de traiter les données personnelles de manière abusive[220].

Les mesures requises doivent faire l'objet d'une évaluation relative en tenant compte du risque d'une violation de la personnalité de la personne concernée, du but et de l'étendue du traitement de données ainsi que de la nature des données traitées[221]. Une sécurité absolue

---

218 Le Conseil des barreaux de la Communauté européenne a publié une liste de mesures préventives contractuelles possibles: Lignes directrices du CCBE sur l'usage des services d'informatique en nuage par les avocats, Bruxelles, 7 septembre 2012, <www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/FR_ITL_20120907_CCBE_guidelines_on_the_use_of_cloud_computing_services_by_lawyers.pdf>, 8; voir également: privatim, la Conférence des Préposé(e) suisses à la protection des données, Aide-mémoire «Risques et mesures spécifiques à la technologie de Cloud computing», <http://www.privatim.ch/wp-content/uploads/2019/02/privatim_Aide-memoire_Cloud_v1.0_20190206-1.pdf>, 3 ss; SURY/GOGNIAT, Revue de l'avocat 2015, *passim*; GRAMIGNA, Datenschutz und Outsourcing, *passim*.

219 FF 1988 II 413, 463 s.

220 SHK-DSG, BAERISWYL DSG 7 N 13.

221 SHK-DSG, BAERISWYL, DSG 7 N 23; EPINEY, § 9 N 53; BSK-DSG/BGÖ, STAMM-PFISTER, DSG 7 N 9; BUNDESAMT FÜR JUSTIZ, Kommentar VDSG, § 6.1.1.

n'est pas exigée[222]. Ce qui est requis, c'est plutôt une analyse des risques au vu de différents critères, soit notamment du but, de la nature et de l'étendue du traitement, des risques pour les personnes concernées ainsi que de l'état de la technique (art. 8 al. 2 OLPD). Le maître d'un fichier, soit d'un portefeuille de données personnelles dont la structure permet de rechercher les données par personne concernée (art. 3 let. g LPD), est tenu, au sens de l'art. 9 OLPD, de prendre des mesures de contrôle particulières: les personnes non autorisées ne doivent pas avoir accès aux installations ou aux systèmes de traitement des données personnelles automatisés et ne doivent pas être autorisées à lire, copier, modifier ou éloigner des supports de données. Lors de la communication de données personnelles, il convient également d'empêcher que les données soient lues, copiées, modifiées ou éloignées de manière non autorisée. En outre, les personnes autorisées ne doivent pouvoir accéder qu'aux seules données dont elles ont besoin pour accomplir leurs tâches. En raison de cette dernière obligation, il doit pouvoir être vérifié quelles personnes ont manipulé les données qui sont enregistrées dans un système automatisé, et comment.

Les mesures techniques requises dépendent directement du système d'information[223] et englobent p. ex. le cryptage (en cas d'enregistrement et de transmission), la gestion des accès, la journalisation et la sauvegarde[224]. Ceci dit, ni la LPD ni l'OLPD ne prescrivent

---

222 SHK-DSG, BAERISWYL DSG 7 N 22; BSK-DSG/BGÖ, STAMM-PFISTER, DSG 7 N 9; EPINEY, § 9 N 53; BUNDESAMT FÜR JUSTIZ, Kommentar VDSG, § 6.1.1.

223 Préposé fédéral à la protection des données et à la transparence (PFPDT), Guide relatif aux mesures techniques et organisationnelles de la protection des données, 5; BSK-DSD/BGÖ, STAMM-PFISTER, DSG 7 N 11; SHK- DSG, BAERISWYL, DSG 7 N 19.

224 SHK-DSG, BAERISWYL DSG 7 N 19; EPINEY, § 9 N 56; ROSENTHAL, in: Rosenthal/Jhöri, DSG 7 N 8; Préposé fédéral à la protection des données et à la transparence (PFPDT), Guide relatif aux mesures techniques et organisationnelles de la protection des données, août 2015, *passim*; il est recommandé de procéder à des sauvegardes sur un disque dur qui est la propriété du cabinet d'avocats, étant donné qu'ainsi une remise est garantie aussi en cas de faillite (SURY/GOGNIAT,

des solutions techniques spécifiques[225]. À titre d'orientation, il est en partie renvoyé aux standards internationaux (p. ex. ISO 27001, ISO 27002, COBIT, BSI 100-1, BSI 100-2, BSI 100-3 et BSI 100-4)[226]. Il n'est pas nécessaire que les mesures techniques et organisationnelles prises soient mises à nu, étant donné que ceci irait à l'encontre de la poursuite des buts de sécurité[227].

Dans le P-LPD, la réglementation existante concernant la sécurité des données est reprise dans une large mesure. En comparaison de l'AP-LPD, on trouve le complément selon lequel les mesures prises doivent permettre d'assurer la sécurité des données (art. 7 al. 2 P-LPD). Cette règle devrait être évidente. Ce qui est en revanche nouveau, c'est le concept de protection des données dès la conception par des mesures techniques («*Privacy by Design*»), selon lequel le responsable du traitement des données est tenu de mettre en place, dès le moment de la planification, les mesures techniques et organisationnelles requises afin que le traitement des données respecte les prescriptions de protection des données et en particulier les principes du traitement des données (art. 6 P-LPD). Selon la teneur de la loi, cette obligation ne concerne cependant pas le tiers qui traite les données[228].

Vu que peu d'avocates et avocats sont en mesure d'évaluer eux-mêmes la sécurité informatique du fournisseur de services de cloud, il peut être recommandé d'impliquer un spécialiste en informatique indépendant[229]. On peut en outre se fier à un système de gestion de qualité du fournisseur de services de cloud certifié (p. ex. ISO 9001 ou ISO 27001), ou à une certification spécifique au droit de la protection

Revue de l'avocat 2015, 204 s., ainsi que CHAPPUIS/ALBERINI, Revue de l'avocat 2017, 341, qui revendiquent que le disque dur se trouve en Suisse). Voir, au sujet de ce qui précède, IV.3.1e) ainsi que III.1.2b)v).

225 BUNDESAT FÜR JUSTIZ, Kommentar VDSG, Abs. 6.1.1.

226 SHK-DSG, BAERISWYL, DSG 7 N 37; BSK-DSG/BGÖ, STAMM-PFISTER, DSG 7 N 21.

227 Cf. ATF 144 I 126, consid. 8.3.6.

228 Ainsi déjà l'art. 18 AP-LPD; ROSENTHAL, Jusletter 20 février 2017, N 11.

229 SURY/GOGNIAT, Revue de l'avocat 2015, 203.

des données (p. ex. GoodPriv@cy, VDSZ:2014, ou encore ePrivacy). La meilleure façon pour les avocates et avocats de remplir leur obligation de surveillance est d'obliger le fournisseur à remplir certains standards en termes de certifications. En outre, le fournisseur de services de cloud peut se voir obliger de communiquer toute perte de certification ou tout autre élément pertinent pour la sécurité des données. Selon le P-LPD, le tiers qui traite les données (sous-traitant) doit annoncer au responsable du traitement tout cas de violation de la sécurité des données en cas de risque probablement accru pour la personnalité ou les droits fondamentaux de la personne concernée (cf. art. 22 al. 3 P-LPD); il prévoit en outre expressément que le sous-traitant ne peut lui-même sous-traiter un traitement à un tiers qu'avec l'autorisation préalable du responsable du traitement (art. 8 al. 3 P-LPD). Ce dernier point correspond cependant aux mesures déjà habituellement prises de nos jours pour contrôler le respect du droit de la protection des données par le sous-traitant[230].

e) Externalisation à l'étranger

i. Communication transfrontière de données

La doctrine dominante, en accord avec la jurisprudence du Tribunal fédéral, est d'avis que si le fournisseur de services de cloud enregistre les données personnelles à l'étranger, on se trouve en présence d'une communication transfrontière de données (art. 6 LPD)[231]. Cependant, certains auteurs sont d'avis qu'il n'y a pas de communication transfrontière parce que le traitement des données sur mandat ne constitue

230 Voir ROSENTHAL, Jusletter 27 novembre 2017, N 53.

231 ATF 144 I 126, consid. 8.3.6; ROSENTHAL, in: Rosenthal/Jhöri, DSG 6 N 7; BSK-DSG/BGÖ, BÜHLER/RAMPINI, DSG 10a N 22d; GRAMIGNA, Datenschutz und Outsourcing, N 20.24; STRAUB, PJA 2014, 914; SCHWANINGER/LATTMANN, Jusletter 11 mars 2013, N 15.

pas une communication de données au sens du droit de la protection des données[232].

Si des données sont transférées vers l'étranger, elles peuvent être, le cas le cas échéant, moins bien protégées juridiquement, ou accessibles à des autorités étrangères. C'est pourquoi l'art. 6 LPD règle séparément la communication transfrontière des données. L'art. 3 let. f définit la communication comme le fait de rendre des données accessibles. La loi énumère à titre exemplatif la consultation, la transmission et la diffusion[233]. Elle inclut tout procédé qui permet à des tiers de prendre connaissance du contenu des données[234]. L'accès à distance depuis l'étranger, p. ex. dans le cadre d'une maintenance à distance du nuage informatique, est de ce fait qualifié de communication transfrontière des données[235]. Est cependant controversée la question de savoir si c'est l'accès possible dans les faits ou plutôt l'accès convenu par contrat qui est déterminant[236]. Étant donné que l'art. 6 LPD entend empêcher la mise en danger de la personnalité de la personne concernée (al. 1), une interprétation basée sur l'évaluation des risques s'impose. Une exclusion contractuelle de la communication à l'étranger semble de ce fait en principe suffisante si l'on ne doit pas présumer que le fournisseur de services de cloud ne se tiendra pas à cette prescription[237].

---

232 SHK-DSG, BAERISWYL, DSG 10a N 43 avec renvoi au N 6; WIDMER, digma 2014, 32.

233 SHK-DSG, RUDIN, DSG 3 N 41.

234 BSK-DSG/BGÖ, BLECHTA, DSG 3 N 77; SHK-DSG, RUDIN, DSG 3 N 41; PASSADELIS, N 6.41.

235 STRAUB, PJA 2014, 914; comp. GRAMIGNA, Datenschutz und Outsourcing, N 20.23; FISCHER/BORNHAUSER, GesKR 2016, 434 s.

236 Concernant l'accès convenu contractuellement: SCHWANINGER/LATTMANN, Jusletter 11 mars 2013, N 19; ROSENTHAL, in: Rosenthal/Jhöri, DSG 6 N 9; similairement: STRAUB, PJA 2014, 914; THALMANN, sic! 2007, 339; se basant sur les possibilités d'accès concrètes: BSK-DSG/BGÖ, BÜHLER/RAMPINI, DSG 10a N 22d.

237 ROSENTHAL, in: Rosenthal/Jhöri, DSG 6 N 9; STRAUB, PJA 2014, 914 n. 82; en rapport avec la question de la sécurité des données, le Tribunal fédéral admet lui

ii. Conditions préalables

Selon l'art. 6 al. 1 LPD, une communication transfrontière n'est admissible que si la personnalité de la personne concernée n'est pas gravement menacée. Selon la loi, une telle situation de mise en danger est donnée si le pays de destination ne dispose pas d'une législation sur la protection des données suffisante. Conformément à l'art. 7 de l'OLPD, le PFPDT publie une liste (non contraignante) des États qui disposent, selon lui, d'une législation assurant un niveau de protection adéquat[238]. Pour ces États, il existe une présomption réfragable selon laquelle ces États garantissent un niveau de protection des données adéquat[239]. Si la personne qui traite les données s'en rapporte de bonne foi à la liste du PFPDT, une communication est admissible[240].

Une communication de données dans des États qui ne figurent pas sur la liste du PFPDT[241] est également possible si l'un des états de fait de l'art. 6 al. 2 LPD est donné. En l'espèce, les éléments suivants sont pertinents: il existe des garanties suffisantes (let. a), la personne concernée a donné son consentement (let. b), un traitement de données personnelles du partenaire contractuel est en relation directe avec le

aussi qu'une garantie juridique suffit, étant donné le fait qu'on ne peut jamais exclure que certaines personnes se comportent de manière illicite (comp. ATF 144 I 126, consid. 8.3.6).

238 PFPDT, État de la protection des données dans le monde, état au 12 janvier 2017, <https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2017/04/staatenliste.pdf.download.pdf/liste_des_etats.pdf>, consulté en dernier lieu le 12 février 2019.

239 OGer Zürich, arrêt du 3 mars 2015, LF140075, consid. E.3.2; PASSADELIS, N 6.44.

240 BSK-DSG/BGÖ, MAURER-LAMBROU/STEINER, DSG 6 N 18b; PFPDT, Transmission des données à l'étranger, 4.

241 Les États membres de l'UE ont tous signé la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel (dite Convention-108; RS 0.235.1), qui interdit fondamentalement aux États membres de limiter entre eux la libre circulation des données à caractère personnel (art. 12 Convention-108). Comme les États-Unis n'ont pas adhéré à la Convention-108, le PFPDT est d'avis qu'ils n'offrent pas un niveau de protection suffisant en matière de protection des données.

contrat (let. c) et la communication a lieu au sein d'une même personne morale ou entre personnes morales réunies sous une direction unique (let. g).

Tandis que pour les données de clients, il est possible de demander une autorisation de divulgation, cette solution n'est pas appropriée pour les données d'une partie adverse ou d'autres tiers, ne serait-ce que pour des raisons de protection du secret. Un cabinet d'avocats devrait de ce fait exiger d'un fournisseur de services de cloud à l'étranger des garanties suffisantes concernant le respect de la protection des données, ou alors plutôt choisir un fournisseur de services de cloud suisse. Le PFPDT a élaboré des contrats-type[242].

f) Excursus: communication aux États-Unis

i. Certification Privacy Shield au titre de garantie suffisante

La question de la communication transfrontière des données aux États-Unis revêt une importance toute particulière au vu des parts de marché importantes tenues par les fournisseurs de services de cloud US-américains. Le PFPDT est d'avis que contrairement à ce qui est le cas pour les États membres de l'UE, les États-Unis ne garantissent de manière générale pas un niveau de protection des données suffisant[243]. C'est pourquoi les sociétés US-américaines peuvent, depuis le 12 avril 2017, se faire certifier selon le Swiss-US Privacy Shield, qui

242 PFPDT, Contrat-type pour l'externalisation (outsourcing) du traitement de données à l'étranger (en anglais), <https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/entreprises/declaration-des-fichiers/contrat-type-pour-l-externalisation--outsourcing--du-traitement-.html>. Le PFPDT doit être informé des garanties fournies à l'étranger (art. 6 al. 3 LDP; GRAMIGNA, Datenschutz und Outsourcing, N 20.26). Pour la communication sur la base de contrats-type du PFPDT, il suffit d'informer ce dernier de manière générale (art. 6 al. 3 OLPD; SHK-DSG, BAERISWYL/BLONSKI, DSG 6 N 51).

243 Cf. PFPDT, Transmission des données à l'étranger, 3; PFPDT, Liste des États, 11; voir également PASSADELIS, N 6.49; GRAMIGNA, Datenschutz und Outsourcing, N 20.26.

remplace l'accord «Safe Harbor» conclu en 2008 entre la Suisse et les États-Unis[244]. Ce faisant, elles s'engagent à appliquer les principes prévus dans le Privacy Shield en matière de traitement de données personnelles. La déclaration d'entreprises US-américaines de respecter ce code de conduite est une garantie suffisante au sens de l'art. 6 al. 2 let. a LPD, qui permet le transfert de données vers les États-Unis[245]. Le Privacy Shield ne permet cependant pas (comme déjà le Safe Harbor Framework) de constater l'adéquation du niveau de protection des données aux États-Unis[246].

C'est à la lumière de l'art. 31 al. 1 let. e LPD que le PFPDT doit examiner la question de savoir si une garantie suffisante au sens de l'art. 6 al. 2 let. a LPD est donnée. Le PFPDT y a jusqu'à présent répondu par l'affirmative. Cependant, la question de savoir si la garantie pourrait être qualifiée d'insuffisante à l'avenir en raison des droits d'accès d'autorités US-américaines est sujette à caution. Ce risque ne peut être exclu, étant donné que c'est justement en grande partie en raison de ces droits d'accès que la CJUE a annulé la décision 2000/520/CE du 26 juillet 2000 rendue par la Commission des Communautés européennes[247] concernant la pertinence de la protection assurée par le

244 Voir à ce sujet la liste du US Department of Commerce: <https://www.privacyshield.gov/list>, consultée en dernier lieu le 7 février 2019.

245 FF 2003 2101, 2129; BSK-DSG/BGÖ, MAURER-LAMBROU/SCHÄFER, DSG 6 N 25; SHK-DSG, BAERISWYL/BLONSKI, DSG 6 N 20; ROSENTHAL, in: Rosenthal/Jhöri, DSG 6 N 49.

246 Voir cependant ROSENTHAL/KAISER, Jusletter 2 novembre 2015, N 3; PASSADELIS, N 6.46; FISCHER/BORNHAUSER, GesKR 2016, 436; SIDLER/VASELLA, sic! 2016, 193, selon lesquels un niveau de protection des données adéquat au sens de l'art. 6 al. 1 LPD est établi.

247 Décision 2000/520/CE: décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la sphère de sécurité et par les questions souvent posées y afférentes, publié par le ministère du commerce des États-Unis d'Amérique, Journal officiel des Communautés européennes L 215/7-47, du 28.08.2000.

Safe Harbour Framework[248]. Au premier plan se trouvait le fait que la Commission avait admis un niveau de protection des données adéquat pour les entreprises certifiées selon la convention Safe-Harbor, sans cependant avoir examiné de manière suffisante la situation juridique aux États-Unis[249]. A entre autres été décisif le fait que le Safe-Harbor Framework était subordonné aux lois US-américaines, ce qui a permis aux autorités US-américaines d'accéder aux données personnelles transmises vers les États-Unis[250]. En revanche, lors de la consultation sur plusieurs années, ayant précédé la mise en place du Swiss-US Privacy Shield, les États-Unis ont informé le PFPDT sur les conditions-cadres juridiques concernant les droits d'accès des autorités[251]. Aussi longtemps que le PFPDT continue de partir – tout à fait à raison – du principe que le Swiss-US Privacy Shield constitue une garantie suffisante, l'éventualité d'un accès par des autorités US-américaines ne remet en question l'admissibilité d'une communication transfrontière des données qu'à partir du moment où existent des éléments concrets permettant de penser qu'un tel accès a systématiquement lieu, ou du moins a lieu dans le cas d'espèce[252].

En ce moment cependant, une procédure est pendante devant la CJUE sur la question de l'admissibilité du transfert de données vers les États-Unis sur la base de garanties suffisantes, et en particulier sur la base de clauses contractuelles standard[253]. Cette procédure pourrait

248 CJUE, arrêt du 6 octobre 2015, C-362/14, *Schrems*.

249 CJUE, arrêt du 6 octobre 2015, C-362/14, *Schrems*, N 83. Voir également RÜPKE/VON LEWINSKI/ECKHARDT, 270.

250 CJUE, arrêt du 6 octobre 2015, C-362/14, *Schrems*, N 87.

251 Voir la documentation de la procédure de consultation: PFPDT, Transmission des données aux États-Unis, <https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland/transmission-des-donnees-aux-etats-unis.html>, consulté en dernier lieu le 26 octobre 2018.

252 STRAUB, PJA 2014, 914 n. 82; cf. MÉTILLE, medialex 2013, 63, selon lequel les garanties de l'art. 6 al. 2 LPD ne peuvent s'étendre aux droits d'accès d'autorités; d'un autre avis, WAGNER/ZWIRNER, 172.

253 CJUE, arrêt C-311/18, *Facebook Ireland/Schrems*, décision non encore rendue.

clarifier des questions ouvertes concernant le transfert de données vers les États-Unis et pourrait – comme ce fut déjà le cas pour le Safe Harbour Framework – avoir une influence sur l'évaluation du Swiss-US Privacy Shield par le PFPDT.

ii. Garanties suffisantes et droits d'accès des autorités (Cloud Act)

L'appréciation du Swiss-US Privacy Shield pourrait en outre être mise en question par le Cloud Act[254] promulgué par le Congrès des États-Unis en mars 2018. Cet acte est une réaction à la décision rendue dans l'affaire Microsoft v. United States, *829 F.3d 197 (2d Cir. 2016)*, dans laquelle le Court of Appeal for the Second Circuit a statué que le Federal Bureau of Investigation (FBI) ne pouvait pas obliger Microsoft à lui remettre des données stockées sur un serveur en Irlande, sur la base du Stored Communications Act (SCA) de 1986[255]. Le Cloud Act règle l'application territoriale des directives («*warrants*») édictées par des autorités US-américaines sur les données enregistrées à l'étranger, ainsi que l'accès des autorités étrangères sur des données de communication enregistrées aux USA[256].

Sur la base du Cloud Act, les autorités US-américaines peuvent accéder à des données enregistrées à l'étranger si celles-ci sont possédées, détenues ou contrôlées par un fournisseur de services de cloud US-américain[257]. Le fournisseur de services de cloud peut cependant contester, sous certaines conditions, un prononcé exigeant de lui qu'il fournisse des données, notamment lorsque celles-ci concernent un citoyen non US-américain et qui n'habite pas aux USA, si l'accès aux données violerait les lois d'un pays avec lequel les USA ont conclu un accord sur le droit d'accès mutuel à des données[258]. Si ces conditions

254 Clarifying Lawful Overseas Use of Data Act.

255 130 Harv. L. Rev. (2016) 769 ss; DASKAL, 71 Stan. L. Rev. Online, 9; STAIGER, 441 s.; VLCEK, 174.

256 DASKAL, 71 Stan. L. Rev. Online, 9; CORDING/GÖTZINGER, CR 2018, 636.

257 GAUSLING, MMR 2018, 579; CORDING/GÖTZINGER, CR 2018, 637.

258 18 U.S.C. § 2703(h)(2)(A–B). CORDING/GÖTZINGER, CR 2018, 637.

préalables sont remplie, le «*warrant*» peut être abrogé par voie judiciaire, si cela semble adéquat au vu d'une pesée des intérêts globale[259]. Le Cloud Act ne prévoit pas d'autres possibilités de contestation, comme en particulier des voies de droit ouvertes à la personne touchée par l'ordre ou des dispositions de protection du secret professionnel de l'avocat[260]. Le secret professionnel suisse et les prescriptions de la LPD ne sont pris en compte dans cette procédure qu'en cas d'accord sur les droits d'accès mutuels aux données conclu entre la Suisse et les USA[261]. Ce changement de paradigme élude consciemment le système établi de l'entraide judiciaire[262].

Comme évoqué ci-dessus, la promulgation du Cloud Act pourrait conduire à ce que le PFPDT modifie son évaluation de l'adéquation de la protection des données auprès des entreprises US-américaines. Cependant, une communication des données aux USA reste probablement admissible aussi longtemps que le PFPDT estime qu'en cas de certification selon le Privacy-Shield, une protection suffisante est encore donnée. Un examen en fonction des risques entrepris au cas par cas ne s'impose que sous l'angle des éléments pertinents en ma-

259 18 U.S.C. § 2703(h)(2)(B)(ii): «*based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed*»; GALBRAITH, AJIL 2018, 489; CORDING/GÖTZINGER, CR 2018, 637. Les facteurs qui doivent être pris en compte dans le cadre de cette pesée des intérêts («*comity analysis*») sont fixés par le 18 U.S.C. § 2703(h)(3).

260 Au sujet de ce qui précède, cf. CORDING/GÖTZINGER, CR 2018, 640.

261 C'est pourquoi il est revendiqué que la Suisse entreprenne des négociations à ce sujet avec les USA (cf. MARKUS STÄDELI, US-Behörden können neu die Herausgabe von Daten auf ausländischen Servern verlangen, NZZ am Sonntag, 15 décembre 2018, <https://nzzas.nzz.ch/wirtschaft/cloud-act-us-behoerden-herausgabe-von-daten-ld.1445117>, consulté en dernier lieu le 17 décembre 2018).

262 DASKAL, 71 Stan. L. Rev. Online, 13. Concernant le système d'entraide judiciaire existant, cf. le Traité du 25 mai 1973 entre la Confédération Suisse et les États-Unis d'Amérique sur l'entraide judiciaire en matière pénale (avec échange de lettres), RS 0.351.933.6.

tière de secret professionnel relatif à des données particulièrement sensibles[263].

3.2 Selon le RGPD

Selon le RGPD, il n'est permis de traiter les données personnelles que si les principes relatifs au traitement sont respectés (art. 5 RGPD) et si l'une des conditions légales de licéité du traitement de données est remplie (art. 6 RGPD). Au premier plan se trouvent ici aussi le consentement par la personne concernée (art. 6 al. 1 let. a RGPD), la sauvegarde des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (art. 6 al. 1 let. f RGPD) et le respect d'une obligation légale (art. 6 al. 1 let. c RGPD).

a) Traitement privilégié du traitement de données sur mandat

La situation juridique concernant l'externalisation du traitement de données selon l'art. 28 RGPD correspond globalement à celle selon la LPD. Celui qui traite les données n'est notamment pas considéré comme un tiers, ce qui montre que le RGPD privilégie lui aussi le traitement de données sur mandat[264]. La doctrine majoritaire est donc d'avis que pour pouvoir faire appel à un sous-traitant, il n'est pas nécessaire de remplir une condition générale régissant la licéité particulière (art. 6 RGPD)[265]. Il faut cependant évoquer une opinion minoritaire parmi la doctrine allemande selon laquelle l'appel à un sous-traitant en matière de traitement de données n'est pas traité de manière privilégiée, mais requiert une condition particulière afin d'être licite[266].

---

263 Voir ci-devant sous III.1.2b)v.

264 PLATH, in: Plath, DSGVO 28 N 3.

265 ECKHARDT, CCZ 2017, 113; SCHMIDT/FREUND, ZD 2017, 16; aboutissant au même résultat: BERTERMANN, in: Ehmann/Selmayr, DSGVO 28 N 4 s.

266 Ainsi p. ex. INGOLD, in: Sydow, DSGVO 28 N 31, qui cependant part du point de vue du motif justificatif en tant qu'autorisation accessoire à la base du traitement,

La condition préalable au privilège du traitement de données par un sous-traitant est que le mandat présente le contenu exigé par l'art. 28 RGPD[267]. Le RGPD dicte en effet le contenu du contrat dans une large mesure. Contrairement à la LPD, le RGPD ne laisse ainsi que peu de libertés au responsable en ce qui concerne la manière dont il remplit ses obligations relatives au traitement de données sur mandat.

Au sens du RGPD – comme au sens de la LPD –, le mandant demeure responsable du respect des prescriptions du droit de la protection des données[268].

b) Devoir d'informer

À la différence de la LPD, le sous-traitant en matière de traitement des données est un destinataire au sens de l'art. 4 n° 9 RGPD lorsque des données sont portées à sa connaissance. Ceci est d'importance en matière de devoir d'informer[269].

Si des données personnelles sont collectées auprès de la personne concernée, le responsable doit lui communiquer, au moment de la saisie, les destinataires ou les catégories de destinataires des données (art. 13 al. 1 let. e RGPD). Le même principe vaut lorsque les données ne sont pas recueillies auprès de la personne concernée (art. 14 al. 1 let. e RGPD). Toujours est-il que dans le dernier cas, il n'existe pas de devoir d'informer lorsque les données sont soumises à une obligation

ce qui, en fin de compte, revient quand même à un traitement privilégié. Voir, au sujet de cette controverse: SCHMIDT/FREUND, ZD 2017, 15.

267 ECKHARDT, CCZ 2017, 113.

268 SHK-DSG, BAERISWYL, DSG 10a N 2; BERTERMANN, in: Ehmann/Selmayr, DSGVO 28 N 11.

269 SCHREIBER, in: Plath, DSGVO 4 N 31; la LPD ne prévoit pas une obligation d'informer sur le traitement de données sur mandat (SHK-DSG, BAERISWYL, DSG 10a N 13). L'art. 17 al. 2 let. e P-LPD prescrit une information sur les destinataires des données personnelles. Le P-LPD ne définit certes par le destinataire, mais étant donné que le but poursuivi est un rapprochement du RGPD (FF 2017 6941, 6970), il serait indiqué de comprendre le tiers qui traite les données sur mandat également comme étant un destinataire.

de secret professionnel réglementée par le droit des États membres (art. 14 al. 5 let. d RGPD). Le devoir d'informer lors de la collecte des données auprès de la personne concernée peut être restreint au sens de l'art. 23 RGPD, selon le droit des États membres[270].

Le devoir d'informer n'est pas un devoir de communication active (sur ce point, la version allemande prête à confusion); les versions anglaise («*provide*»), française («fournir») et italienne («*fornisce*») montrent qu'une simple «mise à disposition» ou «co-livraison» suffit. Corollairement, la personne concernée doit pouvoir accéder aux informations mais ne doit pas être informée activement[271]. Ainsi, il est suffisant de mettre à disposition les informations correspondantes sur le site Internet du cabinet d'avocats[272]. Ce faisant, seule la catégorie de destinataires devrait être désignée dans le sens d'une indication claire de la branche; nommer le fournisseur de services de cloud serait en revanche préjudiciable, étant donné que cela faciliterait les attaques ciblées sur les données.

c) Externalisation à l'étranger

Selon le RGPD, le traitement des données peut être externalisé vers un pays tiers. En raison de l'intégration du RGPD à l'Accord sur l'Espace économique européen (EEE), l'Islande, la Norvège et le Liechtenstein, qui sont membres de l'EEE, ne sont pas considérés

---

270 KAMLAH, in: Plath, DSGVO 14 N 33.

271 LAUE/NINK/KREMER, § 3 N 17; voir également: KAMLAH, in: Plath, DSGVO 12 N 4 et DSGVO 13 N 5.

272 De telles indications figurent sur les sites Internet de cabinets d'avocats européens: voir p. ex. Linklaters, Global Privacy Notice, no 18, version de mai 2018 <https://www.linklaters.com/en/legal-notices/privacy- notice>; Hengeler Mueller, Allgemeine Datenschutzbestimmungen, no IV, <https://www.hengeler.com/de/service/datenschutz/allgemeine-datenschutzbestimmungen/>; Granrut société d'avocats, Protection des données <https://www.granrut.com/-protection-des-donnees-.html>, quoiqu'aucun des cabinet d'avocats ne désigne nommément les destinataires.

comme des États tiers[273]. Selon le RGPD également, la communication de données personnelles à l'étranger n'est pas réglée dans le contexte du traitement de données sur mandat, mais séparément dans le chapitre V (transfert de données à caractère personnel vers des pays tiers, art. 44 ss RGPD)[274]. Le transfert de données à caractère personnel vers des pays tiers n'est en principe autorisé que si la Commission européenne a décidé que le pays tiers concerné garantit un niveau de protection adéquat (art. 45 RGPD)[275], si le responsable ou le sous-traitant a prévu des garanties appropriées, comme p. ex. des clauses contractuelles standard ou des Binding Corporate Rules (art. 47 RGPD), si l'on se trouve en présence d'un cas d'exception. Cela peut p. ex être le cas en présence du consentement de la personne concernée (art. 49 al. 1 let. a RGPD), si le traitement des données personnelles est en lien direct avec un contrat (art. 49 al. 1 let. c RGPD), ou encore si le transfert est nécessaire à l'exercice de la défense de droits en justice (art. 49 al. 1 let. e RGPD).

Selon le responsable suisse, une communication vers un pays tiers ne peut avoir lieu que si les données sont transférées vers un pays non membre de l'EEE. La communication à l'intérieur de la Suisse ne constitue en revanche pas une communication vers un pays étranger, car les données se trouvent déjà dans un pays tiers. Hormis la Suisse, les pays suivants disposent également d'un niveau de protection des données adéquat, selon la Commission européenne: Andorre, l'Argentine, le Canada (cependant uniquement pour les organisations qui traitent les données dans le cadre d'activités commerciales), les Îles Féroé, Guernsey, Israël, l'Île de Man, Jersey, la Nouvelle-Zélande, Uruguay et le Japon. Pour les entreprises domiciliées aux États-Unis,

---

273 Decision of the EEA Joint Committee, no 154/2018 du 6 juillet 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37; cf. ZERDICK, in: Ehmann/Selmayr, DSGVO 44 N 10. La décision du comité de l'EEE est entrée en vigueur le 20 juillet 2018.

274 ECKHARDT, CCZ 2017, 116; ZERDICK, in: Ehmann/Selmayr, DSGVO 44 N 5; SCHRÖDER, in: Kühling/Buchner, DSGVO 45 N 48.

275 ZERDICK, in: Ehmann/Selmayr, DSGVO 44 N 3.

l'adéquation de la protection des données est admise si celles-ci se sont fait certifier selon le EU-US Privacy Shield[276]. Si un fournisseur de services de cloud sis dans un autre pays est choisi, le contrat de cloud devrait contenir des clauses contractuelles standard pour l'externalisation à l'étranger.

[276] European Commission, Adequacy of the protection of personal data in non-EU countries, <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection- personal-data-non-eu-countries_en>, consulté en dernier lieu le 7 septembre 2018. La question de savoir si le bouclier de protection des données UE-États-Unis constitue une garantie suffisante peut prêter à discussion. La Commission européenne et la doctrine dominante qualifient le Privacy Shield de cas spécial de décision d'adéquation (voir également KLUG, in: Gola, DSGVO 45 N 11).

V. Conclusions

L'analyse ci-avant a montré que les avocates et avocats sont autorisés à faire appel à des fournisseur de services de cloud dans le cadre de l'exercice de leur profession. Ce faisant, il faut distinguer entre deux constellations:

Si les avocates et avocats cryptent les données avant de les transmettre au fournisseur de services de cloud et si celui-ci ne possède pas la clé cryptographique correspondante, il n'y a pas de révélation du secret au sens de l'art. 321 CP, parce que le fournisseur de services de cloud ne dispose dans ce cas d'aucune possibilité réaliste de prendre connaissance des informations confidentielles. Étant donné que les données cryptées ne doivent pas être qualifiées de données personnelles, il n'y a pas non plus de traitement de données personnelles par le fournisseur de services de cloud. Dans cette constellation, l'utilisation de services de cloud par les avocates et avocats ne risque ainsi pas de violer le droit pénal ou le droit de la protection des données.

Si les données ne sont pas cryptées par les avocates et avocats mais par le fournisseur de services de cloud, la situation juridique est la suivante:

- Le fournisseur de services de cloud doit être qualifié d'auxiliaire des avocates et avocats, parce qu'il représente une partie de l'unité de fonction «cabinet d'avocats» avec partage du travail; outre les fournisseurs de services de cloud, d'autres personnes externes peuvent faire partie de cette unité de fonction, soit p. ex. un bureau d'administration externe ou un support informatique externe.
- La prise de connaissance d'un secret par des auxiliaires ne constitue pas une révélation au sens de l'art. 321 CP, parce que les auxiliaires font partie du cercle interne de l'organisation des avocates et avocats et peuvent, par définition, prendre connaissance de secrets.

- Lorsque les avocates et avocats font appel à des fournisseurs de services de cloud, cela ne constitue ainsi pas une violation du secret professionnel au sens de l'art. 321 CP.
- Les avocates et avocats sont tenus de choisir avec soin leur fournisseur de services de cloud et de garantir la conservation du secret professionnel par contrat (art. 13 al. 2 LLCA). Ils doivent en outre convenir qu'il n'est permis d'utiliser les données des clients que dans un but d'exécution du contrat et surveiller raisonnablement le respect de cette obligation.
- Le fournisseur de services de cloud doit être qualifié de sous-traitant des avocates et avocats. Le traitement des données qu'il entreprend est licite, car aucune obligation légale de garder le secret n'est ainsi violée. Si les autres directives applicables au traitement des données sur mandat sont également respectées, le fournisseur de services de cloud peut traiter les données de la même manière que ce qui est permis aux avocates et avocats. L'utilisation de services de cloud par les avocates et avocats est ainsi également admissible sous l'angle de la protection des données.
- Si l'avocate ou l'avocat choisit un fournisseur de services de cloud dont le siège se trouve à l'étranger et dont le niveau de protection des données est inadéquat, ou si des techniciens ont accès à des données en texte clair dans le cadre de travaux de maintenance effectués à distance depuis un pays dont le niveau de protection des données est inadéquat, l'avocate ou l'avocat devrait obtenir des garanties suffisantes quant au respect des dispositions du droit de la protection des données applicable. Cela est en particulier nécessaire en cas de collaboration avec des fournisseurs de services de cloud dont le siège se trouve en dehors de l'EEE.

Même si le recours par les avocates et avocats à des fournisseur de services de cloud est admis du point de vue du droit de la protection des données, il est à recommander, au titre de garantie supplémentaire, d'attirer l'attention des clients, dans les contrats de

mandat et les procurations, sur le traitement de données par des fournisseurs de services de cloud. Une telle précision assure non seulement la transparence mais peut, en cas de litige, également faire office de preuve du consentement pour l'implication d'un fournisseur de services de cloud.

Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich

erschienen bei Schulthess Juristische Medien AG Zürich bis 2016
(Vorgänger-Schriftenreihe der ITSL-Reihe)

Band 50 **Datenschutz v. Öffentlichkeitsprinzip**
Erläuterungen zu den Spannungsfeldern am Beispiel des Zürcher Informations- und Datenschutzgesetzes
Weber Rolf H.
Zürich 2010

Band 51 **Online Marketing und Wettbewerbsrecht**
Weber Rolf H./Volz Stephanie
Zürich 2011

Band 52 **Internet-Access-Providing-Verträge mit geschäftlichen und privaten Endkunden**
Eine vertragsrechtliche Analyse nach schweizerischem Recht unter besonderer Berücksichtigung des Rechts der Europäischen Union
Fercsik Schnyder Orsolya
Zürich 2012

Band 53 **Classification of Services in the Digital Economy**
Weber Rolf H.
Zürich 2012

Band 54 **Neuer Regulierungsschub im Datenschutzrecht?**
Weber Rolf H./Thouvenin Florent
Zürich 2012

Band 55 **Die Erzwingung unangemessener Preise im Kartell- und Fernmelderecht – Eine rechtsvergleichende Untersuchung**
Vlcek Michael
Zürich 2013

Band 56 **The Evolution of Global Internet Governance**
Principles and Policies in the Making
Radu Roxana/Chenou Jean-Marie/Weber Rolf. H.
Zürich 2013

Band 57 **The New International Telecommunication Regulations and the Internet**
A Commentary and Legislative History
Hill Richard
Zürich 2013

Band 58 **Trennungsgebot und Internet**
Ein medienrechtliches Prinzip in Zeiten der Medienkonvergenz
Volz Stephanie
Zürich 2014

Band 59 **Big Data und Datenschutz – Gegenseitige Herausforderungen**
Weber Rolf H./Thouvenin Florent (Hrsg.)
Zürich 2014

Band 60 **Realizing a New Global Cyberspace Framework – Normative Foundations and Guiding Principles**
Weber Rolf H.
Zürich 2014

Band 61 **Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme**
Weber Rolf H./Thouvenin Florent (Hrsg.)
Zürich 2015

Band 62 **Datenschutz-Managementsysteme im Aufwind?**
Weber Rolf H./Thouvenin Florent (Hrsg.)
Zürich 2016

Band 63 **Markennutzung bei Keyword-Advertising in Vertriebsverhältnissen**
Rechtsvergleichende markenschutz- und wettbewerbsrechtliche Untersuchung
Neverauskas Giedre
Zürich 2016

Band 64 **Datenpolitik als Rechtsthema**
Agenda für Open Government Data
Weber Rolf H./Laux Christian/Oertly Dominic
Zürich 2016

Veröffentlichungen des Center for Information Technology, Society and Law (ITSL) der Universität Zürich

erschienen bei Schulthess Juristische Medien AG Zürich

Band 1 **Werbung – Online**
Thouvenin Florent/Weber Rolf H. (Hrsg.)
Zürich 2017

Band 2 **Transatlantic Data Protection in Practice**
Rolf H. Weber/Dominic N. Staiger
Zürich 2017

Band 3 **Endorsements and Behavioral Advertising in Social Media under EU, Swiss, and US Law**
Disclosure requirements, personality rights, and data protection
Mane Sargsyan
Zürich 2017