



17. September 2021

Bericht zum US CLOUD Act



Inhaltsverzeichnis

1	Auftrag.....	4
2	Einleitung	4
3	Der <i>CLOUD Act</i>.....	6
3.1	Ausgangslage	6
3.2	Inhalt	6
3.2.1	Wesentlicher materieller Inhalt	6
3.2.2	Möglichkeit des Abschlusses von <i>Executive Agreements</i> mit anderen Staaten auf der Grundlage des <i>CLOUD Acts</i>	7
3.2.2.1	Allgemeines.....	7
3.2.2.2	Materielle Voraussetzungen	8
3.2.2.3	Formelle Voraussetzungen.....	8
3.2.3	Inhalt des <i>Executive Agreements</i>	9
3.2.4	Voraussetzungen für Herausgabeeanordnungen gestützt auf ein <i>Executive Agreement</i>	9
4	Rechtsvergleich.....	10
4.1	<i>Executive Agreement</i> zwischen den USA und dem Vereinigten Königreich.....	10
4.2	EU-E-Evidence vs. <i>US CLOUD Act</i> : Kollision oder Verhandlung?.....	12
4.2.1	E-Evidence-Gesetzgebung der EU.....	12
4.2.2	Gespräche zwischen der EU und den USA	13
4.3	Das Zweite Zusatzprotokoll zum Europarats-Übereinkommen über die Cyberkriminalität (Budapest-Konvention)	15
5	Rechtliche Fragen.....	16
5.1	Territorialität und Souveränität.....	16
5.2	Rechtsnatur der <i>Executive Agreements</i>	18
5.3	Der Begriff «serious crime» (schwere Straftat)	19
5.4	Die Erhebung elektronischer Daten	20
5.4.1	Adressaten.....	20
5.4.2	Datenart	21
5.4.3	Erhebungsmodalitäten.....	22
5.5	Schutz der Grundrechte, insbesondere der Daten und des Privatlebens.....	23
5.5.1	Die EU-Ebene: Verhältnis zwischen dem <i>CLOUD Act</i> und der EU-Datenschutz-Grundverordnung.....	23
5.5.1.1	Vereinbarkeit des <i>CLOUD Acts</i> mit der <i>DSGVO</i>	23
5.5.1.2	Fazit: Risiko des Abschlusses eines <i>Executive Agreements</i> mit den USA im Hinblick auf den Angemessenheitsbeschluss der Schweiz ..	26
5.5.2	Rechtmässigkeit der Bearbeitung und Bekanntgabe von Daten gestützt auf eine Herausgabeeanordnung auf der Grundlage des <i>CLOUD Acts</i> nach Schweizer Recht	29
5.5.2.1	Der vorliegend relevante datenschutzrechtliche Rahmen in der Schweiz.....	29
5.5.2.2	Problematische Aspekte im Hinblick auf die Grundsätze des schweizerischen Datenschutzrechts	30
5.5.2.3	Rechtfertigungsgründe für private Personen bei Verletzungen der Persönlichkeit gemäss Artikel 13 DSG/Artikel 27 nDSG	31

Bericht zum US Cloud Act

5.5.2.4	Vereinbarkeit mit den Anforderungen an grenzüberschreitende Datenbekanntgaben (Art. 6 DSG/Art. 16 und 17 nDSG)	33
5.5.2.5	Weitere aus datenschutz- und grundrechtlicher Sicht problematische Aspekte	34
5.5.2.6	Schlussfolgerung zur Datenschutzkompatibilität eines <i>Executive Agreements</i>	35
5.5.3	Welcher Datenschutz müsste in einem <i>Executive Agreement</i> mit den USA aufgenommen werden?	36
5.6	Vereinbarkeit mit dem schweizerischen Rechtshilferecht	37
5.6.1	Gründe für die Ablehnung eines Rechtshilfeersuchens und Rechtsweggarantie	38
5.6.2	Grundsatz der beidseitigen Strafbarkeit	39
5.6.3	Anspruch auf rechtliches Gehör	39
5.6.4	Aufsichts- und Kontrollbehörde	40
5.6.5	Grundsatz der Spezialität	41
5.6.6	Begrenzung der Zusammenarbeit aus «politischen» Gründen	42
5.6.7	Vereinbarkeit mit der Strafprozessordnung und dem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs	42
5.6.8	Welche «rechtshilferechtlichen» Inhalte müssten in ein <i>Executive Agreement</i> aufgenommen werden?	44
6	Datensicherheit und Entschlüsselung	44
6.1	Gesicherte Übermittlung	44
6.2	Neutral encryption	45
7	Schlussfolgerung	46
8	Weiteres Vorgehen	47
9	Bibliographie	48
10	Abkürzungen	50

1 Auftrag

Im März 2018 haben die USA den sogenannten *Clarifying Lawful Overseas Use of Data Act* (nachfolgend *CLOUD Act*)¹ verabschiedet. Er soll den US-Strafverfolgungsbehörden im Bereich der Verhütung, Ermittlung, Aufklärung oder Verfolgung schwerer Straftaten (*serious crimes*) den Zugriff auf Daten ermöglichen, die von Anbietern von Kommunikationsdiensten (*Communication Service Providers*, CSP) mit Sitz in den USA gespeichert worden sind. Dies unabhängig davon, ob die entsprechenden Daten in den USA oder, etwa über Tochtergesellschaften, im Ausland gespeichert sind, was dem US-Gesetz einen extraterritorialen Anwendungsbereich verleiht.² Der *CLOUD Act* erlaubt zudem unter bestimmten Bedingungen den Abschluss bilateraler Vollzugsvereinbarungen (*Executive Agreements*) zwischen den USA und anderen Staaten. Damit wird Reziprozität hergestellt: Die Strafverfolgungsbehörden des Partnerstaates können mit ihren Ersuchen ebenfalls direkt an US-CSP gelangen, ohne um Rechtshilfe ersuchen zu müssen. Der Partnerstaat toleriert dafür einen entsprechenden Zugriff der US-Strafverfolgungsbehörden auf Daten, die bei CSP auf seinem Territorium gespeichert sind. Vor allem dieser Aspekt hat zur Frage geführt, inwieweit der Abschluss einer solchen Vereinbarung mit den USA für die Schweiz opportun wäre.

Das Bundesamt für Justiz (BJ) ist die schweizerische Zentralstelle im Bereich der Rechtshilfe in Strafsachen.³ In dieser Funktion führt es die Aufsicht über die Anwendung des Rechtshilfegesetzes und ist daneben verantwortlich für die Weiterentwicklung der Rechtsgrundlagen in diesem Bereich. Vor diesem Hintergrund – und aufgrund der Interventionen diverser Akteure aus Privatwirtschaft, Verbänden, Verwaltung und Strafverfolgung beim BJ – hat dieses den vorliegenden Bericht erarbeitet. Dieser soll eine Grundlage für die weiterführende Diskussion mit öffentlichen und privaten Stakeholdern in der Schweiz bilden. Zu diesem Zweck beleuchtet er insbesondere grundsätzliche juristische Fragen, die sich im Zusammenhang mit dem *CLOUD Act* und seiner Vereinbarkeit mit dem Schweizer Recht stellen.

2 Einleitung

Als Folge der Globalisierung spielt auch die zwischenstaatliche Zusammenarbeit in Strafsachen eine immer wichtigere Rolle. Die fortschreitende Digitalisierung sämtlicher Lebensbereiche und im vorliegenden Kontext insbesondere die Erhebung und Übergabe elektronischer Beweismittel stellt diese Zusammenarbeit dabei vor Herausforderungen verschiedenster Art:

- Daten sind *flüchtig* – die herkömmliche Strafrechtshilfe ist oft zu langsam, um diese über Landesgrenzen hinweg rechtzeitig sicherzustellen;
- Daten sind *nicht territorial geprägt* – soll wirklich der *Lageort* für strafbehördliche Zugriffsrechte auf Daten relevant sein, oder nicht eher die Frage, wer und von wo aus sich *Zugriff* auf die Daten verschaffen kann? Noch komplexer wird es bei *blockchain*, wo die Daten physisch nicht mehr an einem eindeutig bestimmbar Ort liegen;
- Daten sind *verschlüsselt* – wie können sie von Strafverfolgungsbehörden, gerade im internationalen Verkehr, wirksam entschlüsselt werden? Gibt es zwischenstaatliche oder globale Regeln?

Es ist offensichtlich: Die zwischenstaatliche Erhebung elektronischer Beweismittel stellt Grundpfeiler der transnationalen Strafverfolgung in Frage. Das Prinzip der Territorialität im

¹ Vollständiger Wortlaut abrufbar unter: <https://www.congress.gov/bill/115th-congress/senate-bill/2383/text>.

² Bereits an dieser Stelle ist darauf hinzuweisen, dass der *CLOUD Act* nur in *Strafverfahren* zur Anwendung kommt. Im Strafverfahren kommt dem Territorialitätsprinzip aus verschiedenen Gründen eine besondere Bedeutung zu. Dazu unten 2. sowie insb. 5.1. Es wird im weiteren Verlauf daher von der *Territorialität insbesondere mit Blick auf das Strafverfahrensrecht* die Rede sein.

³ Vgl. Art. 17 Rechtshilfegesetz (IRSG, SR 351.1) sowie Art. 3 Rechtshilfeverordnung (IRSV, SR 351.11).

Bericht zum US Cloud Act

bisherigen Sinne gerät ins Wanken. Die Verfahren der traditionellen souveränitätsorientierten Strafrechtshilfe sind zu langsam. Man setzt auf direktere Zusammenarbeitsformen, mitunter auf direkte Beteiligung Privater an Strafverfahren im Ausland. Dies ist teilweise aus der Not geboren: Rechtshilfebehörden in Staaten, in denen viele CSP ihren Sitz haben, stossen an die Kapazitätsgrenzen.

Entsprechende Anpassungen im Rechtshilferecht werden zurzeit in verschiedenen Foren, in der EU, aber auch im Europarat und auf UNO-Ebene diskutiert.

Die EU möchte mit einem Vorschlag betreffend Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen vom April 2018 (E-Evidence-Verordnung)⁴ eine erleichterte Zusammenarbeit zwischen ihren Mitgliedstaaten einführen und auf diese Weise die Zusammenarbeit beschleunigen. Im Europarat ist das Komitee für die Cybercrime-Konvention (Budapest-Konvention)⁵, das TC-Y, zurzeit an der Erarbeitung eines Zweiten Protokolls zu dieser Konvention, welches die zwischenstaatliche Zusammenarbeit für mittels Computersystemen begangene Straftaten sowie für den Bereich der elektronischen Beweismittel allgemein regeln soll. Auf UNO-Ebene laufen Vorbereitungen zu einem multilateralen Instrument zur Bekämpfung der Cyberkriminalität.

Während in diesen Foren multilaterale Instrumente diskutiert werden, die auf die Zusammenarbeit zwischen Staaten setzen, haben die USA im März 2018 mit dem *CLOUD Act* auf nationaler Ebene ein Gesetz mit extraterritorialem Anwendungsbereich geschaffen. Das Gesetz soll einerseits den direkten Zugriff der US-Strafverfolgungsbehörden auf Daten von CSP mit Sitz in den USA ermöglichen – unabhängig davon, ob diese Daten in den USA oder im Ausland gespeichert sind – ohne für die im Ausland gespeicherten Daten den Weg über die zwischenstaatliche Rechtshilfe beanspruchen zu müssen. Über bilaterale *Executive Agreements*, die durch den *CLOUD Act* möglich werden, sollen die Strafverfolgungsbehörden der entsprechenden ausländischen Staaten andererseits ohne die Notwendigkeit von Rechtshilfeersuchen ebenfalls Zugang zu den entsprechenden Daten der CSP mit Sitz in den USA erhalten können, indem sie die betreffenden CSP direkt zu deren Herausgabe auffordern. Die ausländischen Staaten können dabei aber keinen Zwang anwenden. Das *Executive Agreement* erlaubt es den CSP, Daten an einen anderen Staat herauszugeben, sie sind jedoch nicht dazu verpflichtet.

Die Schweiz hat mit den USA einen Rechtshilfevertrag abgeschlossen, den Staatsvertrag vom 23. Mai 1973⁶ über gegenseitige Rechtshilfe in Strafsachen (nachfolgend RVUS). Die schweizerischen Behörden erhalten die von einem US-CSP gespeicherten Daten folglich über die internationale Rechtshilfe in Strafsachen. Dieser Weg ist jedoch langwierig, denn das U.S. Department of Justice (DOJ) muss ein entsprechendes Ersuchen prüfen und es der Vollzugsbehörde übermitteln, die dem Ersuchen in der Regel erst nach einem Gerichtsverfahren entsprechen kann und die Beweise schliesslich übermittelt. Erfahrungsgemäss erhalten schweizerische Strafverfolgungsbehörden die ersuchten elektronischen Beweismittel nicht immer – und vor allem nicht immer rechtzeitig. Gleichzeitig hat das DOJ bereits 2016 Weisungen zu den elektronischen Beweismitteln erlassen und fordert die ausländischen Behörden auf, sich direkt an die CSP zu wenden, wenn sie lediglich Abonentendaten (*basic subscriber information*: Name und Adresse, Art und Dauer des in Anspruch genommenen Dienstes, Zahlungsinstrumente inkl. Kreditkarten- und Kontonummern; im Folgenden Bestandsdaten)

⁴ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, COM/2018/225 final – 2018/0108 (COD) vom 17. April 2018.

⁵ Übereinkommen des Europarates über die Cyberkriminalität, SEV 185, SR 0.311.43.

⁶ SR 0.351.933.6

erhalten wollen.⁷ In der Praxis geben gewisse CSP derartige Daten schon heute heraus, während andere die Herausgabe verweigern und auf den offiziellen Weg verweisen.

Auch wenn die Schweiz mit den USA ein *Executive Agreement* abschliesse, bliebe dieser Umstand so bestehen. Weiterhin könnte nur auf dem Rechtshilfeweg um Durchführung von Zwangsmassnahmen ersucht und dieser Zwang gewissermassen über den anderen Staat ausgeübt werden. Die schweizerischen Strafverfolgungsbehörden könnten sich nach Abschluss eines *Executive Agreements* zwar direkt an einen CSP wenden – nunmehr auch für Daten, die über Abonnenteninformationen hinausgehen – dürften aber keine Zwangsmassnahmen anordnen. Würde sich ein CSP weigern, Daten herauszugeben, müsste die Schweiz den Rechtshilfeweg beschreiten, um die Daten zwangsweise erheben zu lassen. Würde ein CSP jedoch kooperieren, verlief die Zusammenarbeit schneller. Die Rechtshilfe mit den USA könnte damit überdies generell entlastet werden und die involvierten Behörden könnten sich auf Fälle konzentrieren, in denen die Zusammenarbeit verweigert wurde oder die nicht in den Geltungsbereich des *CLOUD Acts* fallen. Es gilt die Vermutung, dass sich diejenigen CSP, die schon heute bei der Herausgabe von Bestandsdaten kooperieren, gestützt auf ein *Executive Agreement* aufgrund der klaren Rechtslage weiterhin kooperativ zeigen würden. Weitere CSP würden evtl. zu einer solchen Zusammenarbeit motiviert.

3 Der CLOUD Act

3.1 Ausgangslage

Der *CLOUD Act* ist ein US-amerikanisches Bundesgesetz, welches das Gesetz über gespeicherte Nachrichten, den *Stored Communications Act* (SCA) ergänzt und im März 2018 im Zusammenhang mit einem Gerichtsverfahren in Sachen Microsoft erlassen wurde. Konkret ging es damals darum, dass Microsoft 2013 gestützt auf den SCA von einem US-Richter aufgefordert worden war, in einem Strafverfahren E-Mails und Informationen zu einem von Microsoft gehosteten Account herauszugeben. Microsoft gab die Informationen heraus, die sich auf einem Server in den USA befanden, nicht hingegen die E-Mails, die auf einem Server in Irland gespeichert waren. Dies mit dem Argument, ein amerikanisches Unternehmen könne aufgrund einer derartigen Anordnung nicht zur Herausgabe von auf einem Server im Ausland gespeicherten Daten verpflichtet werden. Das amerikanische Gericht sei nicht zuständig; der SCA habe keine extraterritoriale Wirkung.

Microsoft verlor den Fall in erster Instanz, gewann aber vor dem Berufungsgericht, woraufhin das DOJ die Angelegenheit an den Supreme Court weiterzog. Noch vor dessen Urteil verabschiedete der Kongress den *CLOUD Act*, der den SCA änderte und dem Gesetz die heutige extraterritoriale Wirkung verleiht.

3.2 Inhalt

3.2.1 Wesentlicher materieller Inhalt

Der *CLOUD Act* verpflichtet die CSP mit Sitz in den USA, welche ausserhalb der USA Datenspeicherzentren führen, die Daten, die sich auf ihren Servern befinden, aufzubewahren und den zuständigen US-Strafverfolgungsbehörden auf Ersuchen herauszugeben. Dies unabhängig davon, ob die Daten in den USA oder im Ausland gespeichert sind.⁸ Betroffen sind Gesellschaften nach amerikanischem Recht, d. h. Gesellschaften, die der US-Gerichtsbarkeit unterstehen.⁹ Verlangt wird in diesem Zusammenhang ein Mindestbezug zu den USA (*mi-*

⁷ Für über Abonnentendaten hinausgehende Ersuchen muss lex lata auf jeden Fall der Rechtshilfeweg beschritten werden.

⁸ *CLOUD Act*, §2713. Siehe ebenfalls BISMUTH, S. 683.

⁹ DOJ, «Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act», S. 6 f.

Bericht zum US Cloud Act

nimum contacts), wobei die entsprechende Interpretation und Qualifikation in der Kompetenz der US-Gerichte liegt. Auch Unternehmen mit Holdinggesellschaften, Tochtergesellschaften oder Zweigniederlassungen in den USA können betroffen sein, unter Umständen sogar ausländische Cloud-Anbieter, die in den USA Werbung für ihre Dienstleistung machen. Lediglich denjenigen ausländischen CSP, die keinen solchen Mindestbezug zu den USA haben, werden keine neuen Pflichten auferlegt.

Aus dem *CLOUD Act* selber ergibt sich keine Mindestdauer für die Aufbewahrung von Daten. Im Zusammenhang mit anderen Bestimmungen des US-Rechts, etwa dem SCA, scheint sich aber – mindestens in gewissen Fällen – eine Pflicht zur Aufbewahrung von Daten während 180 Tagen zu ergeben.

Der CSP kann gemäss *CLOUD Act* eine strafbehördliche Anordnung zur Herausgabe von Daten vor einem US-Gericht anfechten (Antrag auf Aufhebung oder Änderung), wenn es sich bei der betroffenen Person nicht um eine sogenannte *US person*¹⁰ handelt und wenn die Bekanntgabe der Daten gegen das Recht eines Staates, welcher ein *Executive Agreement* (vgl. unten, 3.2.2.) mit den USA abgeschlossen hat (*qualifying foreign government*; im Folgenden QFG) zu verstossen droht. Das Gericht berücksichtigt für seinen Entscheid betreffend Aufhebung oder Abänderung der angefochtenen Herausgabeanordnung die Interessen der USA und des QFG, die Beziehung der betroffenen Person zu den USA und zum Staat, der um die Herausgabe der Daten ersucht hat, die Wahrscheinlichkeit einer Strafe und das allfällige Strafmass, die Bedeutung der angeforderten Daten für die Untersuchung und die Interessen der ersuchenden Behörde sowie die Wahrscheinlichkeit, mittels weniger einschneidender Möglichkeiten rechtzeitig und effektiv zu den entsprechenden Daten zu gelangen.¹¹ Falls das Gericht es als notwendig erachtet, kann die sofortige Herausgabe der Daten angeordnet werden, noch bevor der Entscheid zum Aufhebungs- oder Abänderungsantrag gefällt wurde.¹²

Weder der ausländische Staat noch die betroffene Person selber kann sich dem Ersuchen der US-Behörden widersetzen, sondern ausschliesslich der CSP.

3.2.2 Möglichkeit des Abschlusses von *Executive Agreements* mit anderen Staaten auf der Grundlage des *CLOUD Acts*

3.2.2.1 Allgemeines

Der zweite Teil des *CLOUD Acts* ermöglicht es den USA, unter gewissen Voraussetzungen mit anderen Staaten *Executive Agreements* abzuschliessen, auf deren Grundlage die zuständigen Behörden beider Staaten die CSP mit Sitz im jeweils anderen Staat direkt um Informationen oder auf ihren Servern gespeicherte Daten ersuchen können. Gestützt auf entsprechende *Executive Agreements* können die CSP die ihnen vom anderen Staat direkt zugeschickte internationale Herausgabeanordnung (*international production order*, im Folgenden Herausgabeanordnung) direkt beantworten. Die CSP können aber vom ausländischen Staat wie erwähnt nicht zur Herausgabe der Daten gezwungen werden. Eine Herausgabeanordnung ersetzt also die Rechtshilfe nicht – dies gilt zumindest dann, wenn der CSP nicht freiwillig kooperiert.

¹⁰ *CLOUD Act*, § 2713 (h) (2) (A)

¹¹ *CLOUD Act*, § 2713 (h) (3) (A)-(H)

¹² *CLOUD Act*, § 2713 (h) (4)

Bericht zum US Cloud Act

3.2.2.2 Materielle Voraussetzungen

Gemäss *CLOUD Act* muss der Staat, der mit den USA ein *Executive Agreement* aushandeln will, gewisse Mindestvoraussetzungen erfüllen:¹³

Seine nationale Gesetzgebung muss mit Bezug auf den Schutz der Privatsphäre und der bürgerlichen Freiheiten im Hinblick auf die Sammlung von Daten und seine Aktivitäten, die Gegenstand des *Executive Agreements* sind, «robuste» materielle und verfahrensmässige Garantien bieten, die mit denjenigen in den USA vergleichbar sind. Er muss namentlich über angemessene Gesetzesbestimmungen im Bereich der Cyberkriminalität und der elektronischen Beweismittel verfügen. Dies kann unter anderem dadurch nachgewiesen werden, dass er Vertragspartei der Budapest-Konvention ist.

Allgemein muss der betreffende Staat die Rechtsstaatlichkeit sowie den Grundsatz der Nicht-diskriminierung achten und sich an die geltenden internationalen Verpflichtungen im Bereich der Menschenrechte halten, darunter den Schutz vor willkürlichen und rechtswidrigen Eingriffen in das Privatleben, das Recht auf ein faires Verfahren, auf Meinungsäusserungs-, Vereinigungs- und Versammlungsfreiheit, das Verbot von willkürlichen Festnahmen und Inhaftierungen sowie von Folter und grausamer, unmenschlicher oder erniedrigender Behandlung oder Strafe.

Die Regierungsstellen, die auf der Grundlage des *Executive Agreements* um Daten ersuchen dürfen, müssen ein rechtlich klar definiertes Mandat haben und insbesondere im Bereich der Erhebung, Speicherung, Verwendung und Bekanntgabe der Daten über klare gesetzliche Vorgaben und Verfahren verfügen. Es müssen ausreichende Mechanismen bestehen, mit denen die Transparenz hinsichtlich der Erhebung und Verwendung elektronischer Daten durch die fremde Regierung nachgewiesen werden kann.

Der betroffene Staat muss sodann nachweisen, dass er bestrebt ist, den weltweiten freien Datenverkehr sowie den offenen, freien und vernetzten Charakter des Internets zu fördern und zu schützen.¹⁴ Und schliesslich muss er reziproke Rechte für den Zugriff auf die Daten gewährleisten, das heisst, den CSP mit Sitz in seinem Hoheitsgebiet erlauben, Ersuchen der US-Strafverfolgungsbehörden direkt nachzukommen.

Eine auf das *Executive Agreement* gestützte Herausgabeanordnung darf nicht direkt auf derartige *US persons* abzielen. Der betroffene Staat muss daher geeignete Massnahmen ergriffen haben, um dies zu vermeiden. Der *CLOUD Act* enthält sodann eine ganze Liste mit weiteren Voraussetzungen, die eine Herausgabeanordnung erfüllen muss.¹⁵

3.2.2.3 Formelle Voraussetzungen

In den USA ist die Exekutive für den Abschluss der *Executive Agreements* zuständig. Der US Attorney General entscheidet zusammen mit dem Aussenminister, ob der andere Staat die Voraussetzungen für den Abschluss erfüllt, und übermittelt die schriftliche Bestätigung dem

¹³ *CLOUD Act*, § 2523 (b)

¹⁴ *CLOUD Act*, §2523 (b) (1) (B) (vi)

¹⁵ *CLOUD Act*, § 2523 (b) (2) und (3)

Bericht zum US Cloud Act

US-Kongress.¹⁶ Das derart zertifizierte *Executive Agreement* kann von amerikanischer Seite in Kraft treten, falls der Kongress nicht innert 180 Tagen Widerspruch erhebt.¹⁷

Die Vereinbarung wird jeweils für eine bestimmte Zeit abgeschlossen. Der Staat, der mit den USA eine derartige Vereinbarung abschliesst, muss sich dabei einer periodischen Evaluation durch die USA unterziehen.¹⁸

3.2.3 Inhalt des Executive Agreements

Ein erster Teil des *Executive Agreements* müsste allgemeine Bestimmungen wie Definitionen, anwendbares Recht, Form und Inhalt der Ersuchen, zuständige Behörden und Bestimmungen zum Datenschutz enthalten.

Eine der wichtigsten Definitionen ist diejenige von *serious crime* (schwere Straftaten). Gemäss *CLOUD Act* müssen sich die auf der Grundlage eines *Executive Agreements* gestellten Ersuchen auf die Verfolgung schwerer Straftaten beschränken. Darunter sind neben Terrorismus, der im *CLOUD Act* explizit erwähnt wird, etwa Mord oder Kindesentführung zu verstehen. Es muss auch bestimmt werden, welche Daten unter das *Executive Agreement* fallen können, nämlich ob ausschliesslich Daten, die bereits gespeichert worden sind, betroffen sind, oder ob auch in Echtzeit abgefangene Daten in Frage kommen. Der Begriff des CSP und was ein solcher genau umfasst, muss schliesslich ebenfalls definiert werden.

In der Schweiz sind der Zusammenarbeit im Rechtshilferecht verschiedene Grenzen gesetzt. Insoweit als der *CLOUD Act* eine Form der internationalen Zusammenarbeit in Strafsachen ermöglicht, wäre zu prüfen, in welchem Umfang bei einer allfälligen Aushandlung eines *Executive Agreements* die gemäss schweizerischem Recht wesentlichen Prinzipien für die Zusammenarbeit in den Text einfliessen. Allfällige spezifische Ausschlussgründe müssten explizit in ein solches *Executive Agreement* hineinverhandelt werden.

Ein allfälliges *Executive Agreement* muss sodann auch technische Bestimmungen über die Übermittlung von Informationen und die Speicherung von Daten enthalten. Es muss geregelt werden, dass die Übermittlung von Daten und Informationen über einen sicheren Kanal erfolgt. Auch die Anforderungen bezüglich der Speicherung von Daten in einem gesicherten System und dem Zugang zu diesen Daten im ersuchenden Staat müssen festgelegt werden.

In formeller Hinsicht muss das *Executive Agreement* Bestimmungen zu den einzuhaltenden Verfahren, unter anderem zur Frage von Beschwerden oder Aufhebungsanträgen im Zusammenhang mit Herausgabeanordnungen enthalten.

3.2.4 Voraussetzungen für Herausgabeanordnungen gestützt auf ein Executive Agreement

Gemäss *CLOUD Act* müssen Herausgabeanordnungen, die sich auf ein *Executive Agreement* stützen, verschiedene Mindestvoraussetzungen erfüllen.¹⁹

Bei der Person, deren Daten von der ausländischen Herausgabeanordnung betroffen sind, darf es sich nicht um eine *US person* handeln, d. h. sie darf weder Staatsangehörige der

¹⁶ *CLOUD Act*, §2523 (b)

¹⁷ *CLOUD Act*, §2523(d) (2)

¹⁸ *CLOUD Act*, §2523(b) (4) (J)

¹⁹ *CLOUD Act*, § 2523 (b) (3)

Bericht zum US Cloud Act

USA sein noch dort ihren Wohnsitz, oder im Fall einer Gesellschaft, ihren Sitz dort haben.²⁰ Im umgekehrten Fall dürften die US-Strafverfolgungsbehörden nicht die Herausgabe von Daten von Personen mit schweizerischer Staatsangehörigkeit, mit Wohnsitz in der Schweiz oder einer Gesellschaft mit Sitz in der Schweiz verlangen. Der ausländische Staat darf somit unter dem *Executive Agreement* weder Anordnungen zustellen, welche direkt *US persons* zum Ziel haben, noch solche, die zwar eine *non US person* betreffen, die aber zum Ziel haben, Informationen über eine *US person* zu erhalten, und umgekehrt.²¹ Wie Tochtergesellschaften von Schweizer Unternehmen, die nach US-Recht gegründet wurden, in diesem Zusammenhang behandelt würden, scheint nicht klar. Wenn es um Personen geht, die vom Anwendungsbereich des *Executive Agreements* ausgeschlossen sind, muss auf dem Weg der Rechtshilfe um die entsprechenden Daten ersucht werden.

Die Herausgabeanordnung muss sich auf ein *serious crime* beziehen – ein Begriff, der im *Executive Agreement* zu definieren wäre (vgl. Ziff. 5.3). Sie muss zudem namentlich im Einklang mit dem Recht des anordnenden Staates sein, eine Person, eine Adresse, einen persönlichen Gegenstand oder ein anderes Identifizierungsmerkmal angeben und durch nachvollziehbare und glaubwürdige Fakten gerechtfertigt sein (keine sog. *Fishing expeditions*), von einem Gericht oder einer anderen unabhängigen Behörde überprüft werden können und, im Fall von Abhörungsanordnungen, zeitlich befristet und verhältnismässig sein.²²

In der Anordnung muss nicht nachgewiesen werden, dass eine *probable cause* vorliegt,²³ was die Zusammenarbeit gerade im Verhältnis mit den USA erleichtert und zu einer starken Entlastung der schweizerischen Strafverfolgungsbehörde führen würde.

4 Rechtsvergleich

4.1 *Executive Agreement* zwischen den USA und dem Vereinigten Königreich

Das Vereinigte Königreich (UK) ist der erste und bisher einzige Staat, mit dem die USA ein *Executive Agreement* gestützt auf den *CLOUD Act* ausgehandelt haben. Der genaue Wortlaut des Instruments, das am 3. Oktober 2019 unterzeichnet wurde, aber nach wie vor nicht in Kraft ist, ist online abrufbar.²⁴ Als erstes derartiges Instrument ist es von besonderer Bedeutung, da es die wesentlichen Grundzüge auch künftiger *Executive Agreements* festlegen dürfte.

Es handelt sich um eine relativ kurze Vereinbarung, die in verschiedenen Punkten auf andere Instrumente verweist, namentlich die Budapest-Konvention, das Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten²⁵ sowie den Vertrag über die Rechtshilfe in Strafsachen zwischen den USA und UK. Seine Struktur ist derjenigen eines Rechtshilfevertrags in Strafsachen ähnlich. Es enthält Definitionen, Zweck, Grenzen, Bestimmungen zum Datenschutz usw.

Die Definitionen der für das *Executive Agreement* wichtigen Begriffe umfassen insbesondere diejenigen der zuständigen Behörde, des CSP, der Daten sowie des *serious crime* (Art.

²⁰ Gemäss *CLOUD Act*, § 2523 (a) (2) "incorporated in the United States".

²¹ *CLOUD Act*, § 2523 (b) (3) (A) und (B)

²² *CLOUD Act*, § 2523 (b) (3) (D)

²³ DOJ, «Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act», S. 8.

²⁴ Abrufbar unter: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf. Gemäss Auskunft der britischen Botschaft in Bern ist ein Inkrafttreten des Abkommens evtl. Ende Sommer 2021 zu erwarten.

²⁵ Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten, ABl. L 336 vom 10. Dezember 2016, S. 3.

Bericht zum US Cloud Act

1). Die Anordnungen zur Offenlegung oder Herausgabe ausserhalb des eigenen Staates gespeicherter Daten (nachfolgend Anordnung) müssen dem nationalen Recht der anordnenden Vertragspartei entsprechen (Art. 5 Abs. 1). Das nationale Recht der Vertragspartei, in der sich der CSP befindet, muss demgegenüber nicht zwingend eingehalten werden. Die Anordnung muss vor eine Justizbehörde oder unabhängige Behörde der anordnenden Vertragspartei gebracht werden können, damit diese deren Vereinbarkeit mit ihrem nationalen Recht überprüfen kann (Art. 5 Abs. 2). Das bedeutet, dass ein Provider mit Sitz in den USA, der eine Anordnung von UK erhält, den Fall an die britischen Behörden ziehen kann. Für kleinere CSP kann es jedoch schwierig sein, in einem anderen Staat, insbesondere in den USA, zu klagen. Das *Executive Agreement* sieht eine Art Zentralbehörde vor, welche die Vereinbarkeit der Anordnung mit dessen Text überprüfen muss, bevor sie an den CSP gesandt wird (Art. 5 Abs. 6). Demnach muss eine Behörde, die Informationen von einem CSP erhalten will, zuerst diese Zentralbehörde konsultieren.

Wenn ein CSP der Ansicht ist, dass die erhaltene Anordnung nicht dem *Executive Agreement* entspricht, so muss er dies zuerst bei den zuständigen Behörden des Staates geltend machen, der die Anordnung übermittelt hat, d. h. des Staates, in dem er gerade nicht seinen Sitz hat. Wenn er mit seiner Einrede nicht durchdringt, kann sich der CSP auch an die zuständigen Behörden in seinem Sitzstaat wenden (Art. 5 Abs. 11). Beide Behörden suchen nach einer einvernehmlichen Lösung. Sollte die Behörde des Sitzstaats zum Schluss gelangen, dass die Anordnung nicht dem Abkommen entspricht, kann sie die Behörde des anderen Staates darüber informieren, und das Abkommen ist auf die Anordnung nicht anwendbar (Art. 5 Abs. 12). Es scheint damit ein Verfahren vorgesehen zu sein, wonach die Zentralbehörde des Sitzstaates in letzter Instanz darüber entscheiden kann, ob eine Anordnung dem *Executive Agreement* entspricht.

Die gestützt auf das *Executive Agreement* erhaltenen Daten dürfen nicht ohne Zustimmung des Staates, in dem der CSP seinen Sitz hat, an einen Drittstaat weitergegeben werden (Art. 8 Abs. 2). Wird um Informationen zu einer Person ersucht, die sich ausserhalb des Territoriums der anordnenden Vertragspartei befindet und kein Staatsbürger der selbigen ist, muss der Drittstaat, dessen Angehöriger diese Person ist, darüber in Kenntnis gesetzt werden.²⁶

Wenn die erhobenen Daten Fälle betreffen, die in den USA zur Verhängung der Todesstrafe oder in UK zur Verletzung der Meinungsäusserungsfreiheit gemäss amerikanischem Verständnis führen könnten, muss die Zentralbehörde des anderen Staates einbezogen werden und der Verwendung der Daten zustimmen (Art. 8 Abs. 4). Ohne Zustimmung des anderen Staates dürfen die gestützt auf den *CLOUD Act* in UK beschafften Daten nicht verwendet werden, um in den USA die Todesstrafe auszusprechen, und dürfen die in den USA beschafften Daten nicht verwendet werden, um in UK eine Strafe in Verbindung mit der Verletzung der Meinungsäusserungsfreiheit zu verhängen²⁷ – es bestehen also entsprechende Veto-rechte.²⁸

In Bezug auf den persönlichen Geltungsbereich des *Executive Agreements* besteht eine Asymmetrie zwischen den USA und UK. Britische Anordnungen dürfen sich nicht auf *US persons* beziehen. Das umfasst sowohl Personen mit Wohnsitz/Sitz in den USA, unabhängig

²⁶ DASKAL, SWIRE, «The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards». Art. 5 des Abkommens.

²⁷ CHRISTAKIS, «21 Thoughts and Questions about the UK-US *CLOUD Act* Agreement», pt. 15–16; Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America in Access to Electronic Data for the Purpose of Countering Serious Crime, pt. 19–20.

²⁸ DASKAL, SWIRE, «The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards».

Bericht zum US Cloud Act

von ihrer Staatsangehörigkeit, als auch amerikanische Staatsangehörige mit Wohnsitz im Ausland. Amerikanische Anordnungen hingegen dürfen sich grundsätzlich auf britische Staatsangehörige beziehen. Bloss Personen, die sich *auf britischem Territorium* befinden, sind vom Geltungsbereich des Abkommens ausgenommen – unabhängig von deren Staatsangehörigkeit. Dahinter scheinen Grundsätze des EU-Rechts (Unionsbürgerschaft) zu stehen.²⁹

Die CSP werden auch durch das *Executive Agreement* nicht verpflichtet, den Ersuchen der Behörden des anderen Staates zu entsprechen. Wenn ein CSP die Auskunft verweigert, kommt das Gesetz des ersuchenden Staates zur Anwendung.³⁰ Wenn eine Zwangsmassnahme erforderlich ist, ist grundsätzlich internationale Rechtshilfe in Strafsachen zu beantragen. In Bezug auf die Verschlüsselung ist das Instrument neutral. Es verpflichtet die Provider nicht zur Entschlüsselung.³¹

Die Einhaltung des *Executive Agreements* wird von den Parteien ein Jahr nach Inkrafttreten und daraufhin in regelmässigen Abständen überprüft (Art. 12 Abs. 1). Jede Partei muss der anderen überdies jährlich einen Bericht zu dessen Anwendung unterbreiten (Art. 12 Abs. 4). Es soll während fünf Jahren in Kraft sein und kann dann aufgehoben oder auf unbestimmte Zeit verlängert werden.

4.2 EU-E-Evidence vs. US CLOUD Act: Kollision oder Verhandlung?

4.2.1 E-Evidence-Gesetzgebung der EU

Auf EU-Ebene laufen aktuell ebenfalls Bestrebungen zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln (sog. E-Evidence). Es soll innerhalb der EU ein Rechtsrahmen geschaffen werden, der die Sicherung von und den Zugang zu elektronischen Beweismitteln in grenzüberschreitenden Fällen für die Polizei und die Justizbehörden erleichtern und beschleunigen soll. Die Idee für eine E-Evidence-Gesetzgebung ist zurückzuführen auf die Terroranschläge in Brüssel im März 2016 und der daraus entstandenen Forderung in der EU, neue Wege zu finden, um elektronische Beweismittel schneller und wirksamer zu sichern und verstärkter mit Drittländern und im europäischen Hoheitsgebiet tätigen Dienstleistungserbringern zusammenzuarbeiten.³²

Im April 2018 legte die Kommission zwei Gesetzgebungsvorschläge zur E-Evidence vor: einen Vorschlag für eine Verordnung über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen³³ und einen Vorschlag für eine Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren.³⁴

Der Verordnungsvorschlag führt für die betroffenen Behörden verbindliche Europäische Herausgabebeanordnungen (EPOC) und Europäische Sicherungsanordnungen (EPOC-PR) ein.

²⁹ Abrufbar unter: <https://www.hrw.org/news/2019/10/29/groups-urge-congress-oppose-us-uk-cloud-act-agreement>.

³⁰ Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America in Access to Electronic Data for the Purpose of Countering Serious Crime, pt. 18.

³¹ CHRISTAKIS, «21 Thoughts and Questions about the UK-US CLOUD Act Agreement», pt. 14; DASKAL, SWIRE, «The UK-US CLOUD Act Agreement is Finally Here, Containing New Safeguards».

³² Gemeinsame Erklärung der EU-Minister für Justiz und Inneres und der Vertreter der EU Organe zu den Terroranschlägen vom 22. März 2016 in Brüssel vom 24. März 2016, abrufbar unter: <https://www.consilium.europa.eu/de/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/>.

³³ Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabebeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen vom 17. April 2018, COM(2018)225 final.

³⁴ Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren vom 17. April 2018, COM(2018)226 final.

Bericht zum US Cloud Act

Diese Instrumente sollen parallel zu den derzeit bestehenden Rechtsinstrumenten bestehen, welche der Erleichterung von Beweiserhebungen im Hoheitsgebiet eines anderen Mitgliedstaats dienen, wie z. B. der Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen («EEA-Richtlinie»)³⁵.

Die Europäische Herausgabeordnung soll den Behörden ermöglichen, mit einer richterlichen Anordnung digitale Daten anzufordern, die von einem CSP in einem anderen EU-Staat gespeichert wurden und als Beweismittel in strafrechtlichen Ermittlungen oder Strafverfahren erforderlich sind. Diese Idee baut im Wesentlichen darauf auf, dass jeder CSP, der in der EU Dienstleistungen erbringen will, dort einen Vertreter (sog. *legal representative*) bestimmen muss, der Zugang zu den Daten des gesamten Unternehmens hat. Die vorgeschlagene Richtlinie sieht einheitliche Regeln für die Bestellung von solchen Vertretern vor. Die Behörden (Polizei oder Staatsanwaltschaft eines EU-Mitgliedstaates) können für die Zustellung und Ausführung von Anordnungen direkt auf diesen Vertreter zugreifen, und zwar unabhängig davon, wo in der EU dieser Vertreter seinen Sitz hat. Der Kontakt erfolgt auch hier nicht mehr zwischen den Behörden eines Staates, sondern zwischen einer Behörde und einem Unternehmen, also einer privaten Stelle.³⁶ Die betroffenen Unternehmen müssen die Daten innerhalb von wenigen Stunden bis Tagen (10 Tage, in dringenden Fällen innerhalb von 6 Stunden) herausgeben.

Die Europäische Sicherungsanordnung richtet sich – wie die Europäische Herausgabeordnung – an den Vertreter eines CSP, der sich ausserhalb des Rechtssystems des Anordnungsmitgliedstaates befindet. Mit der Sicherungsanordnung können die CSP verpflichtet werden, Daten mit Blick auf ein späteres Herausgabeersuchen zu sichern.³⁷

Aktuell befindet sich das Geschäft im sog. Trilog, d. h. dem politischen Bereinigungsprozess zwischen der EU-Kommission, dem Rat der EU und dem Europäischen Parlament.

4.2.2 Gespräche zwischen der EU und den USA

Die EU-Kommission beantragte im Februar 2019 ein Verhandlungsmandat zur Aufnahme von Gesprächen mit den USA über ein Abkommen zwischen der Europäischen Union und den USA über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen.³⁸ Im Juni 2019 ermächtigte der Rat der Europäischen Union die Kommission zur Aufnahme entsprechender Verhandlungen im Namen der EU.³⁹

Grund für die Aufnahme von Gesprächen mit der USA ist primär die E-Evidence-Gesetzgebung der EU. Obwohl die Vorschläge zu E-Evidence CSP betreffen, die Dienstleistungen auf dem EU-Markt erbringen, besteht die Gefahr, dass die darin vorgesehenen Verpflichtungen mit Rechtsvorschriften von Drittstaaten kollidieren. Die Entwürfe zur E-Evidence-Gesetzgebung der EU enthalten zwar kollisionsrechtliche Bestimmungen. Da aber die in strafrechtlichen Verfahren im EU-Raum relevantesten CSP ihren Sitz in den USA haben und somit der Hoheitsgewalt der USA unterstehen, sollte ein Abkommen zwischen der EU und den USA all-

³⁵ Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen, ABl. L 130 vom 1.5.2014, S. 1.

³⁶ TSILIKIS, S. 169 f. und 172 f.

³⁷ Zum Ganzen siehe Ausführungen im Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, Erwägung 47.

³⁸ Empfehlung der Europäischen Kommission für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen vom 5. Februar 2019, COM(2019) 70 final.

³⁹ Abrufbar unter: <https://www.consilium.europa.eu/de/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-E-Evidence-in-criminal-matters/>.

Bericht zum US Cloud Act

fällige Kollisionen von Verpflichtungen im Verhältnis zwischen beiden Systemen vermeiden. Ziel der EU ist es, mit einem völkerrechtlichen Abkommen Rechtskollisionen insbesondere in Bezug auf Inhaltsdaten zu vermeiden und den Zugang zu elektronischen Beweismitteln zu beschleunigen. Da das geltende amerikanische Recht US-CSP die Beantwortung von Ersuchen ausländischer Strafverfolgungsbehörden hinsichtlich Inhaltsdaten untersagt und Strafverfolgungs- und Justizbehörden aus der EU derzeit Schwierigkeiten haben, entsprechende Daten mithilfe von Rechtshilfeersuchen zu beschaffen, soll ein Abkommen einen effizienteren Rechtsrahmen für diese Behörden schaffen und eine direkte Zusammenarbeit mit CSP ermöglichen. Ein Abkommen zwischen der EU und den USA würde aus EU-Sicht also primär das Ziel und die Wirksamkeit der Vorschläge zu E-Evidence ergänzen, insbesondere in Bezug auf Inhaltsdaten, die sich im Besitz eines US-CSP in den USA befinden. Mit Bezug auf Nichtinhaltsdaten fordern die amerikanischen Behörden die Strafverfolgungs- und Justizbehörden der EU wegen der steigenden Zahl der Rechtshilfeersuchen wie erwähnt bereits heute auf, diese Daten direkt bei den US-CSP anzufordern (vgl. Einleitung). In dieser Hinsicht erlaubt das US-Recht CSP mit Sitz in den USA, solche Ersuchen direkt zu beantworten, verpflichtet sie jedoch nicht dazu. Ein Abkommen zwischen der EU und den USA soll daher auch beim Zugang zu Nichtinhaltsdaten, die sich im Besitz eines US-CSP befinden, mehr Rechtssicherheit schaffen.⁴⁰

Bei den Verhandlungen zwischen der EU und den USA handelt es sich gemäss informellen Informationen damit um keine eigentlichen «CLOUD-Act»-Verhandlungen. Ziel ist es vielmehr, eine Brücke zwischen dem amerikanischen *CLOUD Act* und der E-Evidence-Gesetzgebung zu bauen. Während in diesem Prozess die EU versucht, ihr E-Evidence-System durchzusetzen, möchten die USA dem System des *CLOUD Acts* zum Durchbruch verhelfen. Da die beiden Systeme genau umgekehrte Ansätze gewählt haben (USA: extraterritoriale Wirkung; EU: Verpflichtung des CSP bzw. des Vertreters zur «territorialen» Anwesenheit), sind sie nicht ohne Weiteres kompatibel. Ziel ist es jedoch, dass auf beiden Seiten des Atlantiks Behörden direkt an CSP gelangen können, unabhängig davon, auf welchem Kontinent sie den Firmensitz haben. Durch das Abkommen sollen die rechtlichen Aspekte des Zugangs zu Inhalts- und Nichtinhaltsdaten, die sich im Besitz von CSP in der EU und in den USA befinden, denselben Vorschriften unterliegen.

Bisher haben gemäss informellen Informationen vier Verhandlungsrunden stattgefunden. Ein wesentlicher Teil der Gespräche betraf den Datenschutz. In diesem Punkt hat die Kommission erklärt, dass das Rahmenabkommen zwischen der EU und den USA zum Datenschutz ergänzt werden muss.⁴¹ Zu zahlreichen Punkten bestehen noch grosse Differenzen. Allerdings dürfte es für die Kommission nicht einfach sein, in den Verhandlungen substantiell weiterzukommen, solange die Trilogverhandlungen zum E-Evidence-Paket vom nicht abgeschlossen sind. Denn ihre Verhandlungsposition hängt wesentlich vom Ergebnis dieses Verfahrens ab.⁴² Die Form des Abkommens ist noch offen. Es wird sich zudem in den bestehenden Rechtsrahmen einfügen müssen,⁴³ und das Verhältnis zwischen den verschiedenen Rechtsquellen wird noch zu klären sein.

⁴⁰ Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen vom 5.2.2019, COM(2019) 70 final.

⁴¹ Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten (ABl. L 336, 10.12.2016, S. 3–13).

⁴² Report of the Commission services on the second round of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 6 November 2019, abrufbar unter: <https://www.statewatch.org/news/2019/nov/eu-council-usa-E-Evidence-13713-19.pdf>.

⁴³ Siehe z. B. Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Rechtshilfe sowie die Budapest-Konvention und die bilateralen Übereinkommen mit den Mitgliedstaaten.

Bericht zum US Cloud Act

Die Verhandlungen mit den USA werden zudem beeinflusst von den parallel dazu laufenden Verhandlungen im Europarat über ein Zweites Zusatzprotokoll zur Budapest-Konvention, die ähnliche Fragen zum Gegenstand haben und ähnliche Schwierigkeiten mit sich bringen, da die EU in den Verhandlungen zu diesem Protokoll einen grossen Einfluss hat (siehe Ziff. 4.3). Die Inhalte dieses Protokolls können damit direkte Auswirkungen auf die Verhandlungen zwischen der EU und den USA haben.⁴⁴

Ist das Abkommen einmal ausgehandelt, muss das Europäische Parlament dem Wortlaut des Abkommens noch zustimmen und der Rat einen Beschluss zum Abschluss des Abkommens fassen.

4.3 Das Zweite Zusatzprotokoll zum Europarats-Übereinkommen über die Cyberkriminalität (Budapest-Konvention)⁴⁵

Dem gleichen Grundziel wie die bereits erwähnten Instrumente und Vorhaben dient das Zweite Zusatzprotokoll zur Budapest-Konvention, das zurzeit im Europarat ausgearbeitet wird: Auch dieses Instrument soll dazu dienen, Strafverfolgungsbehörden den Zugang zu elektronischen Beweismitteln zu erleichtern. Es soll die künftige Zusammenarbeit zwischen den Vertragsstaaten – darunter auch die USA, in denen viele der am meisten genutzten CSP ihren Sitz haben – bei der Verfolgung von *cyber-enabled criminality* effizienter gestalten und beschleunigen. Es soll insbesondere dazu dienen, Strafverfolgungsbehörden den Zugang zu elektronischen Beweismitteln zu erleichtern, vor allem wenn sich diese im Ausland befinden. Die Zusammenarbeit mit ausländischen Providern soll erleichtert werden.

Entsprechend enthält das Protokoll unter anderem Bestimmungen, welche die Vertragsparteien verpflichten sollen, in ihrem nationalen Recht Regelungen für die direkte Zusammenarbeit mit CSP auf dem Gebiet einer anderen Vertragspartei zu schaffen. Dabei geht es um Zugriff auf Informationen zu Domain-Namen oder Nutzerdaten, Verfahren zur beschleunigten Herausgabe von Nutzerinformationen und Verbindungsdaten sowie die beschleunigte Herausgabe gespeicherter Daten in Notfällen. Weitere Bestimmungen enthalten die Voraussetzungen für die Zusammenarbeit sowie Bestimmungen bezüglich Ausschlussgründen, insb. Datenschutz.

Die mit dem Zweiten Zusatzprotokoll verfolgten Ziele, die auf einen gewissen Abbau und eine «Auslagerung» rechtsstaatlicher und verfahrensmässiger Garantien zugunsten einer rascheren Kooperation ausgerichtet sind, stehen allerdings im Widerspruch zum Anspruch, dass das Übereinkommen von möglichst vielen Staaten weltweit ratifiziert werden soll. Der Europarat hat die Schwelle für einen Beitritt von Drittstaaten zur Budapest-Konvention erheblich gesenkt. So werden auch Staaten zum Beitritt eingeladen, die teilweise nicht willens oder in der Lage sind, grundlegende Menschenrechte und Verfahrensgarantien sicherzustellen.

Konkret besteht mit diesem Protokoll die Gefahr, dass im Rahmen der Strafverfolgung eine erleichterte Zusammenarbeit mit Staaten geschaffen wird, ohne dass gleichzeitig ein genügender verfahrensrechtlicher Schutz und genügende Garantien im Bereich der Menschenrechte gewährleistet sind. Die zuweilen zitierte «*community of trust among the States Parties*» ist nur schwerlich denkbar in einem stetig erweiterten Kreis von Vertragsstaaten, von denen nicht alle die aus schweizerischer Sicht grundlegenden Verfahrensgarantien und elementaren Grundrechte einhalten können oder wollen.

⁴⁴ Factsheet der Europäischen Kommission vom 5. Februar 2019, Fragen und Antworten: Mandat für das Zweite Zusatzprotokoll zum Budapest-Übereinkommen, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/MEMO_19_865 (Stand 1.7.2020).

⁴⁵ Übereinkommen des Europarates über die Cyberkriminalität (Budapest-Konvention), SEV 185, SR 0.311.43; <https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185>.

Die Arbeiten des Europarates hätten im Dezember 2020 abgeschlossen werden sollen, was angesichts der teilweise erheblichen Differenzen zwischen den Delegationen (z. T. grundsätzlich divergierende Betrachtungsweisen der US-Delegation und von Australien, Kanada, Japan einerseits sowie der EU andererseits) jedoch nicht möglich war. Es ist fraglich, ob die Schweiz angesichts des beschriebenen Dilemmas zwischen Universalisierung des Protokolls und Vereinfachung der Zusammenarbeit einerseits und Aspekten des Rechtsschutzes andererseits eine rasche Unterzeichnung des Protokolls anstreben wird. Ein behutsames Vorgehen mit regelmässiger Analyse der kurz- und mittelfristigen Auswirkungen und Erfahrungen mit dem neuen Protokoll erscheint zum heutigen Zeitpunkt angezeigt.

Ergänzend ist darauf hinzuweisen, dass auch auf globaler Ebene im UNO-Rahmen Vorarbeiten hin zu einer globalen Cyber-Crime-Konvention unternommen werden. Das anhand der Budapest-Konvention erörterte Spannungsfeld zeigt sich hier natürlich umso akzentuierter. Die Arbeiten sind allerdings zurzeit noch zu wenig weit gediehen, weshalb im vorliegenden Bericht nicht weiter darauf eingegangen wird.

5 Rechtliche Fragen

5.1 Territorialität und Souveränität

Das Territorialitätsprinzip ist ein zentraler Pfeiler des Völkerrechts, gerade auch mit Blick auf Abgrenzungsfragen im Bereich der strafrechtlichen Zuständigkeit. Es weist eine enge Verbindung zur staatlichen Souveränität auf. Staatssouveränität beinhaltet positiv betrachtet die Kompetenz der Staaten, sich rechtlich und strukturell selbst zu organisieren und internationale Verträge abzuschliessen, und negativ betrachtet das Verbot, sich in interne Angelegenheiten anderer Staaten einzumischen (Interventionsverbot⁴⁶). Aus dem Territorialitätsprinzip und den durch das Gebot der staatlichen Nichteinmischung gesetzten Grenzen leitet sich das Verbot für die Staaten ab, durch ihre Rechtsetzung oder tatsächliche Handlungen die Souveränität und die territoriale Integrität anderer Staaten zu verletzen.

Im *Lotus-Entscheid*⁴⁷ von 1927, dem ein Frankreich und die Türkei betreffender Zwischenfall auf hoher See zugrunde lag, hielt der Ständige Internationale Gerichtshof (StIGH) fest, dass das Territorialitätsprinzip über das eigene Hoheitsgebiet hinausgehende Rechtsanwendungen zumindest dann nicht ausschliesst, wenn sie völkerrechtlich nicht explizit verboten sind. In einem Entscheid von 1992 nahm auch das Bundesgericht darauf Bezug: «[D]ie extraterritoriale Anwendung des eigenen Rechts [wird] auch im Völkerrecht und im internationalen Strafrecht nicht a priori als unzulässig betrachtet [...]. Vielmehr darf sich die interne Gesetzgebung nach vorherrschender Lehre und Praxis auch auf extraterritoriale Sachverhalte beziehen, wenn eine eindeutige Binnenbeziehung dieser Sachverhalte zum inländischen Recht besteht»⁴⁸.

Der internationale Handel, die globale Mobilität und namentlich auch die moderne Kommunikation mit weltweit verfügbaren, jederzeit abrufbaren Daten stellen das Territorialitätsprinzip vielleicht nicht grundsätzlich in Frage. Sie vervielfachen aber die Berührungspunkte und das Kollisionspotenzial zwischen den verschiedenen staatlichen Rechtsordnungen. Umso wichtiger sind klare Abgrenzungen zwischen völkerrechtlich zulässigen, über das eigene Territorium hinauswirkenden Rechtsanwendungen und verbotener extraterritorialer Kompetenzüberschreitung. Völkerrechtlich anerkannte Anknüpfungspunkte sind namentlich die territoriale Anknüpfung (z. B. Aufenthalt oder Wohnsitz einer Person, Sitz oder Niederlassung eines

⁴⁶ Art. 2 Abs. 7 UNO-Charta, SR 0.120.

⁴⁷ Publications de la Cour Permanente de Justice Internationale (CPJI), Recueil des Arrêts, Série A – No. 10, S. 18 f., Arrêt No. 9: Affaire du «Lotus» du 7 septembre 1927.

⁴⁸ BGE 118 Ia 137 E. 2b S. 142.

Bericht zum US Cloud Act

Unternehmens, Ausführungsort einer Tätigkeit) oder die persönliche Anknüpfung (z. B. Staatsangehörigkeit einer handelnden oder von einer Handlung betroffenen Person). In Einzelfällen, etwa zur Wahrung der eigenen Sicherheit bei Angriffen oder akuten Bedrohungen sowie zur Wahrung allgemein anerkannter, fundamentaler Interessen der internationalen Gemeinschaft wie beispielsweise zur Bekämpfung schwerster Verbrechen im Rahmen des Universalitätsprinzips, kann auch eine Anknüpfung an ein bestimmtes materielles Verhalten ausreichen.

Auch das Strafrecht knüpft an diesen völkerrechtlichen Grundsätzen an.⁴⁹ Als letztes und schärfstes Mittel, das einer demokratischen Ordnung zur Verteidigung ihrer Werte zur Verfügung steht,⁵⁰ ist der Bezug zu Souveränität und Territorialität im Strafrecht jedoch besonders eng. Im Unterschied beispielsweise zu einem Zivilverfahren kann im Strafverfahren nie von der Mitwirkung der Parteien – insbesondere nicht der beschuldigten Person – ausgegangen werden. Vielmehr kann diese den Grundsatz, dass sie sich nicht selbst beschuldigen muss,⁵¹ für sich in Anspruch nehmen. Beweiserhebung im inquisitorischen Strafprozessrecht kontinentaleuropäischer Staaten ist daher grundsätzlich eine staatliche Aufgabe. Der *Staat* ermittelt – so zumindest die Fiktion – die Wahrheit.⁵² Strafrechtliche Beweiserhebung ist daher mit direkten Zugriffsmöglichkeiten für die Strafverfolgungsbehörden verbunden. Aufgrund der zentralen Rolle staatlicher Organe bei strafrechtlicher Beweiserhebung ist zu ihrer Vornahme grundsätzlich der Staat zuständig, *auf dessen Territorium die Beweismittel liegen*. Die Belegenheit einer Sache spielt im Rahmen von Strafverfahren daher eine zentrale Rolle: Zuständig für die Erhebung von Sachbeweisen ist grundsätzlich die Strafverfolgungsbehörde am *Lageort*. Dieses Prinzip wurde bisher im Grund auch auf Daten übertragen – diese sind ebenfalls am «Lageort» zu erheben.

Der *CLOUD Act* hält sich nur beschränkt an diese Prinzipien. Sein Geltungsbereich ist in räumlicher, zeitlicher und inhaltlicher Hinsicht sehr weit gefasst (siehe Ziff. 3.2). Unter das Gesetz fallen alle CSP mit Sitz in den USA. Damit findet das Gesetz auf Daten Anwendung, die von ausländischen CSP ausserhalb der USA gespeichert oder kontrolliert werden, wenn diese CSP in den USA Geschäftsniederlassungen betreiben. Allenfalls könnte es auch schon genügen, wenn nicht-US-CSP aus dem Ausland auf den US-Markt ausgerichtete Dienstleistungen anbieten.⁵³ Einerseits können US-Strafverfolgungsbehörden somit gestützt auf den *CLOUD Act* Daten erheben, die nicht in den USA liegen. Andererseits können sich die amerikanischen Behörden an Unternehmen wenden, die ihren Sitz nicht in den USA haben und insofern nicht zwingend ihrer Gerichtsbarkeit unterstehen. Insbesondere diese zweite Tatsache kann hinsichtlich der Territorialität als problematisch erachtet werden. Gemäss dem *CLOUD Act* können sich die amerikanischen Behörden direkt an eine Privatperson (den CSP) im Hoheitsgebiet des anderen Staates wenden, ohne dass der Staat darüber informiert wird. Zudem stehen dem ausländischen CSP als Rechtsmittel nur Verfahren in den USA zu Verfügung, dessen Recht er nicht unbedingt kennt, sodass er benachteiligt sein könnte.

Dadurch wird das völkerrechtliche Territorialitätsprinzip zwar nicht grundsätzlich in Frage gestellt, doch der Geltungsbereich des *CLOUD Acts* kann zu extraterritorialen *strafrechtlichen*

⁴⁹ Vgl. dazu die strafrechtliche Zuständigkeit begründenden Prinzipien der Territorialität, der Personalität sowie des Weltrechtsprinzips.

⁵⁰ Vgl. m.w.H. FRANZ RIKLIN, Schweizerisches Strafrecht, Allgemeiner Teil I, Verbrechenlehre, Zürich 2007, §4 N 7.

⁵¹ Vgl. Art. 6 Abs. 1 EMRK sowie Art. 113 Abs. 1, Art. 140, Art. 158 Abs. 1 Bst. b, Art. 262 Abs. 2 und Art. 265 Abs. 2 Bst. a StPO.

⁵² Vgl. Art. 2 bzw. Art. 6 StPO.

⁵³ Vgl. dazu den Bericht zuhanden der französischen Nationalversammlung «Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale» vom 26. Juni 2019, Ziff. 1.2.4.2.1, S. 29 f.; abrufbar unter: https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2019/06/rapport_gauvain.pdf.

Kompetenzkonflikten führen. Die Frage der «Tolerierung» eines solchen extraterritorialen Zugriffs auf Daten müsste in einem allfälligen *Executive Agreement* geregelt werden.

5.2 Rechtsnatur der *Executive Agreements*

Der *CLOUD Act* sieht vor, dass die USA mit anderen Staaten *Executive Agreements* abschliessen können (vgl. dazu. 3.2.2). Gestützt auf solche Vereinbarungen sollen sich Strafverfolgungsbehörden aus Staaten mit (aus US-Sicht) rechtsstaatlich-demokratischer Grundordnung sowie mit den USA vergleichbaren Datenschutzstandards und Verfahrensgarantien direkt an die CSP in den USA wenden können, um Daten zur strafrechtlichen Verfolgung von *serious crimes* zu erhalten. Gleichzeitig tolerieren diese Partnerstaaten den Zugriff der US-Strafverfolgungsbehörden auf Daten bei CSP in ihrem Territorium. Die Datenherausgabe erfolgt in einem solchen Fall ohne Rechtshilfeverfahren direkt zwischen dem CSP und dem jeweils «ersuchenden» Staat.

Der *CLOUD Act per se* (also auch ohne zusätzliches *Executive Agreement*) bietet den US-Strafverfolgungsbehörden, wie dargelegt wurde, die Möglichkeit, in einem US-Strafverfahren Zugang zu den Daten zu erhalten, die im Besitz eines US-CSP irgendwo auf der Welt gespeichert sind. Vor diesem Hintergrund ist die Möglichkeit, mit anderen Staaten unter gewissen Voraussetzungen *Executive Agreements* abzuschliessen, ein wichtiges Element zur Förderung der Akzeptanz des *CLOUD Acts*. Die USA verlassen sich dabei auf die Attraktivität ihres CSP-Standorts und bieten ihren Partnern Reziprozität an, um so den Mangel des *CLOUD Acts* mit Blick auf den Respekt des völkerrechtlichen Territorialitätsprinzips zu heilen. Auch der Mangel hinsichtlich Rechtsschutz wird adressiert: Wenn in den USA ein Verfahren gegen einen ausländischen Staatsangehörigen eröffnet wird, können die amerikanischen Behörden gestützt auf den *CLOUD Act* grundsätzlich um die Herausgabe von dessen Daten ersuchen. Es besteht jedoch eine Ausnahme betreffend die Bekanntgabe der Daten eines ausländischen Staatsangehörigen, mit dessen Heimatstaat die USA ein *Executive Agreement* abgeschlossen haben. Liegt ein solches vor, können die CSP gemäss dem *CLOUD Act* einen Aufhebungs- oder Änderungsantrag stellen, wenn ihr Kunde nicht eine *US person* ist und wenn die Datenbekanntgabe das Recht des QFG verletzen könnte. Ein *Executive Agreement* könnte folglich für Schweizer Staatsangehörige und Personen, die der schweizerischen Gerichtsbarkeit unterstehen, einen gewissen Schutz bieten. Wenn die Gefahr besteht, dass die Bekanntgabe gegen schweizerisches Recht verstösst, könnten die CSP in den USA eine Klage einreichen, um die Rechte der betroffenen Personen zu schützen. Demnach würde ein *Executive Agreement* einen gewissen Schutz vor einem unbefugten Zugriff der US-Strafverfolgungsbehörden auf (Personen-)Daten in der Schweiz bieten. Wie dieser Schutz ausgestaltet sein müsste, damit er übergeordnetem Schweizer Recht zu genügen vermöchte, wird unten bei 5.5 und 5.6 erörtert.

In formeller Hinsicht bemerkenswert ist, dass der *CLOUD Act* als US-Bundesgesetz selbst bereits die Voraussetzungen für einen Abschluss, den materiellen Geltungsbereich sowie wesentliche Inhalte der *Executive Agreements* beschreibt. Dennoch handelt es sich bei den *Executive Agreements* formal betrachtet um bilaterale Staatsverträge, die unter die Wiener Vertragsrechtskonvention (WVK)⁵⁴ fallen. Auf diese Verträge und ihre Auslegung finden somit die allgemeinen völkerrechtlichen Regeln und die daraus entwickelte Praxis Anwendung und nicht etwa amerikanisches Recht oder die amerikanische Rechtsprechung. Die Anwendung amerikanischen Rechts wäre nur möglich, wenn ein *Executive Agreement* direkt auf amerika-

⁵⁴ Wiener Übereinkommen über das Recht der Verträge vom 23. Mai 1969, SR 0.111.

Bericht zum US Cloud Act

nisches Recht verweisen würde. Die zwischen den USA und dem Vereinigten Königreich abgeschlossene Vereinbarung tut das nicht.⁵⁵ Sie enthält eigenständige Pflichten und Rechte, die nicht aus nationalem Recht abgeleitet sind. Die Bestimmungen des *CLOUD Act*, die sich mit den *Executive Agreements* befassen, sind aus einer völkerrechtlichen Perspektive daher eher «Handlungsanweisungen» des US-Gesetzgebers an die eigene Regierung.

Staatsverträge bedürfen in der Schweiz der Zustimmung der Bundesversammlung. Der Bundesrat unterzeichnet sie und unterbreitet sie der Bundesversammlung zur Genehmigung. Nach einem positiven Beschluss ratifiziert er sie (Art. 184 Abs. 2 der Bundesverfassung [nachfolgend BV]⁵⁶). Ausnahmsweise darf der Bundesrat Staatsverträge allein abschliessen. Das ist der Fall, wenn sich seine Zuständigkeit aus einem Gesetz oder völkerrechtlichen Vertrag ergibt (Art. 166 Abs. 2 BV). In diesen Fällen wird ihm von der Bundesversammlung die Vertragsschlusskompetenz mittels Delegation eingeräumt. Ausserdem kann der Bundesrat Staatsverträge selbständig abschliessen, wenn es sich um Verträge von beschränkter Tragweite handelt (so Art. 7a Abs. 2 des Regierungs- und Verwaltungsorganisationsgesetzes [RVOG]⁵⁷).

Ein *Executive Agreement*, wie es im *CLOUD Act* geregelt ist, wäre kein Vertrag von beschränkter Tragweite. Eine solche Vereinbarung, die es schweizerischen und amerikanischen Behörden ermöglichen würde, Daten direkt bei den CSP einzuholen, würde die datenschutzrechtlichen und verfahrensrechtlichen Garantien der betroffenen natürlichen oder juristischen Personen wesentlich berühren. Zudem enthält die schweizerische Gesetzgebung im Bereich des Datenschutzes zwar eine Delegationsnorm zugunsten des Bundesrates (Art. 67 nDSG), ein *Executive Agreement* wie dasjenige gestützt auf den *CLOUD Act* liesse sich aber nicht darunter subsumieren. Es ist damit davon auszugehen, dass gemäss Artikel 184 Absatz 2 BV die Genehmigung der Bundesversammlung nötig wäre.

Der Abschluss eines *Executive Agreements* hätte erhebliche Auswirkungen auf die Kantone und die Gemeinden. Zum einen sind Daten betroffen, die in den Geltungsbereich des kantonalen Datenschutzrechts fallen. Zum anderen geht es um strafrechtliche Verfahren, die mehrheitlich in die Zuständigkeit der Kantone fallen. Auch wenn der Bund gestützt auf seine umfassende Kompetenz in auswärtigen Angelegenheiten (Art. 54 Abs. 1 BV) Staatsverträge auch in Bereichen abschliessen kann, die in die Kompetenz der Kantone fallen, muss er diese zwingend einbeziehen, wenn er aussenpolitische Entscheide fällen will, «die ihre Zuständigkeiten oder ihre wesentlichen Interessen betreffen» (Art. 55 Abs. 1 BV). Dann muss der Bundesrat die Kantone rechtzeitig und umfassend informieren und ihre Stellungnahmen einholen (Art. 55 Abs. 2 BV). Ein solcher Fall wäre beim Abschluss eines *Executive Agreements* voraussichtlich gegeben.

5.3 Der Begriff «serious crime» (schwere Straftat)

Die *Executive Agreements* können als Grundlage für die Beschaffung von Informationen zum Zweck der Verhütung, Ermittlung, Aufklärung oder Verfolgung von *serious crimes* dienen.⁵⁸ Welche Delikte im Sinne des *Executive Agreements* solche *serious crimes* darstellen, kann etwa mittels Deliktskatalog oder Nennung einer Mindeststrafandrohung im *Executive Agreement* verdeutlicht werden.

⁵⁵ Agreement between the United Kingdom and the USA on Access to Electronic Data for the Purpose of Countering Serious Crime vom 3. Oktober 2019, Fn. 21.

⁵⁶ SR 101

⁵⁷ SR 172.010

⁵⁸ DOJ, «Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act», S. 5.

Bericht zum US Cloud Act

Die erstgenannte Variante (Deliktskatalog) birgt dabei den Nachteil, dass sie statisch ist. Es ist eine stete Aktualisierung vorzunehmen und im Falle von Gesetzesanpassungen könnten Widersprüche entstehen.

Die zweite Variante (Nennung einer Mindeststrafandrohung) ist dynamisch, beinhaltet jedoch einen potenziell weiter gefassten Geltungsbereich (z. B. alle Verbrechen und Vergehen). Dabei zeigt sich die Herausforderung, dass die Straftaten in den verschiedenen Staaten nicht unbedingt gleich qualifiziert werden. Während eine Handlung im einen Staat mit einer hohen Strafe bedroht ist, wird sie vielleicht im anderen Staat milder oder gar nicht bestraft. Es stellt sich also die Frage, ob in beiden Staaten das Kriterium der *serious crimes* erfüllt sein müsste und man also an einer entsprechend «qualifizierten» beidseitigen Strafbarkeit anknüpft – oder ob man den Zugriff auf Daten bei einem CSP selbst dann tolerieren würde, wenn die Tat im eigenen Staat nicht entsprechend strafbar wäre.

Angesichts des nach wie vor ausgesprochen grossen Engagements der USA im Kampf gegen den Terrorismus ist absehbar, dass die umfassende Abdeckung der Zusammenarbeit bei «Terrorismus» auf jeden Fall ein US-Ziel für ein allfälliges *Executive Agreement* wäre. Dies ist vor dem Hintergrund der möglicherweise engeren Definition der terroristischen Organisation im revidierten Artikel 260^{ter} StGB⁵⁹ nicht unproblematisch. Besonders deutliche und politisch heikle unterschiedliche Bewertungen lägen voraussichtlich im Bereich der *fiskalischen Delinquenz* vor. Der generelle Ausschluss der *Steuerhinterziehung* (vgl. Art. 3 Abs. 3 IRSG) ist kaum mit den Interessen der USA vereinbar. Dies dürfte ausserdem für den Bereich der *Ehrverletzungsdelikte* gelten. In den USA gilt eine sehr weitgehende Redefreiheit (*freedom of speech*), die grundsätzlich auch Hassrede (*hate speech*) umfasst, soweit darin nicht ein unmittelbarer Aufruf zu Gewalt gesehen wird. Viele solcher Reden wären in der Schweiz längst strafbar, insbesondere unter dem Tatbestand der Rassendiskriminierung (Art. 261^{bis} StGB).

Es zeichnet sich damit ab, dass es herausfordernd wäre, zwischen der Schweiz und den USA einen gemeinsamen Standard für den Begriff der «*serious crimes*» zu finden.

5.4 Die Erhebung elektronischer Daten

Das Ziel des *CLOUD Acts* bzw. eines *Executive Agreements* ist es, elektronische Daten grenzüberschreitend erhebbar zu machen. Eine wichtige Frage ist daher, bei wem welche Daten wie erhoben werden können. So kann beurteilt werden, ob die Erhebungsmodalitäten kompatibel sind oder gegebenenfalls angepasst werden müssen.

In den USA wie in der Schweiz richtet sich die Gesetzgebung an Fernmeldediensteanbieter und damit zusammenhängende Dienstleistungserbringer.

5.4.1 Adressaten

Die US-Gesetzgebung unterscheidet zwischen Anbietern von elektronischen Kommunikationsdiensten (*electronic communication services*) und jenen von Ferncomputerdiensten (*remote computing services*). Ein elektronischer Kommunikationsdienst ist jedes Dienstleistungsangebot, das dem Benutzer erlaubt, drahtgebundene oder elektronische Mitteilungen (*wire or electronic communications*) zu senden oder zu empfangen.⁶⁰ «Drahtgebunden» sind

⁵⁹ Vgl. BBl 2020 7891.

⁶⁰ «[A]ny service which provides to users thereof the ability to send or receive wire or electronic communications» (18 USC § 2510(15)).

Mitteilungen mittels der menschlichen Stimme.⁶¹ Elektronische Mitteilungen beinhalten vereinfacht gesagt den Transfer von Daten unter Ausschluss von Mitteilungen mittels menschlicher Stimme.⁶² Ferncomputerdienste umfassen die öffentliche Bereitstellung von Speicherkapazität oder Prozessorleistung über einen elektronischen Kommunikationsdienst.⁶³

In der Schweiz wird vereinfacht gesagt unterschieden zwischen Anbietern von Fernmeldediensten («FDA») und abgeleiteten Kommunikationsdiensten. Fernmeldedienste beinhalten die «fernmeldetechnische Übertragung von Informationen für Dritte»,⁶⁴ während sich die abgeleiteten Kommunikationsdienste «auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen».⁶⁵ Nach der Botschaft des Bundesrates meint die Einwegkommunikation z. B. das Hochladen bzw. Online-Bearbeiten von Dokumenten (z. B. Google Docs oder Microsoft Office online). Abgeleitete Kommunikationsdienste sind demnach u. a. Webhosting-Angebote, Plattformen für den Dokumentenaustausch und nicht zuletzt Cloud-Dienste.⁶⁶ Die Mehrwegkommunikation bezieht sich auf die Interaktion zwischen Nutzern, wie sie z. B. E-Mail, eine Chatfunktion oder eine Voice-Over-IP-Anwendung wie Skype ermöglicht.⁶⁷

Die Ausgangslage in beiden Rechtsordnungen (USA und Schweiz) zeigt sich vor diesem Hintergrund zwar nicht als «identisch», doch immerhin auch nicht so unterschiedlich, dass eine Einigung auf eine gemeinsame Definition der Adressaten in einem *Executive Agreement* als unmöglich erschiene.

5.4.2 Datenart

Bei der Datenart bestehen ebenfalls Parallelen. Grundsätzlich wird auf beiden Seiten des Atlantiks zwischen Bestands-, Rand- und Inhaltsdaten unterschieden. Bestandsdaten (*basic subscriber information*)⁶⁸ im Sinne des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs BÜPF geben Auskunft über den Kunden und das Vertragsverhältnis mit dem Provider.⁶⁹ Randdaten im Sinne des BÜPF oder Metadaten (*transactional data*) beschreiben vereinfacht gesagt insbesondere, wer wann mit wem wie kommuniziert

⁶¹ ««[W]ire communication» means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce» (18 USC § 2510(1)). ««[A]ural transfer» means a transfer containing the human voice at any point between and including the point of origin and the point of reception» (18 USC § 2510(18)).

⁶² ««[E]lectronic communication» means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include— (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds» (18 USC § 2510(12)).

⁶³ «[T]he term «remote computing service» means the provision to the public of computer storage or processing services by means of an electronic communications system» (18 USC § 2711(2)).

⁶⁴ Art. 3 Bst. b Fernmeldegesetz (FMG, SR **784.10**).

⁶⁵ Art. 2 Bst. c Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR **780.1**).

⁶⁶ So ausdrücklich die Botschaft, BBl **2013** 2708.

⁶⁷ BBl **2013** 2708; anzumerken ist, dass derzeit eine Revision des FMG läuft, welche auch eine Revision des Art. 2 BÜPF enthält, mit dem Ziel, dieses System anzupassen und insb. die Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste genauer zu definieren.

⁶⁸ Dazu gehören insbesondere Name, Adresse, Art und Dauer des in Anspruch genommenen Dienstes, Zahlungsinstrumente inkl. Kreditkarten- und Kontonummern: 18 USC § 2703(c)(2).

⁶⁹ Vgl. die Definition in Art. 18 Abs. 3 der Budapest-Konvention: «[A]lle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Diensteanbieter über Teilnehmer seiner Dienste vorliegen, mit Ausnahme von Verkehrsdaten oder inhaltsbezogenen Daten, und durch die Folgendes festgestellt werden kann:

a. die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Massnahmen und die Dauer des Dienstes;

b. die Identität des Teilnehmers, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen;

c. andere Informationen über den Ort, an dem sich die Kommunikationsanlage befindet, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen.»

hat.⁷⁰ Inhalt (*content*) schliesslich bezeichnet die Substanz der eigentlichen Nachricht in Wort oder Schrift. Je näher der staatliche Eingriff an den Kern der Kommunikation, d. h. an den Inhalt kommt, desto intrusiver und daher rechtfertigungsbedürftiger ist er. In den USA und in der Schweiz können Bestandsdaten ohne gerichtliche Genehmigung erhoben werden. Die Erhebung von Rand- und Inhaltsdaten benötigt in beiden Ländern eine gerichtliche Genehmigung. In der Schweiz stellt die Erhebung von Rand- oder Inhaltsdaten eine Zwangsmassnahme dar, die Erhebung von Bestandsdaten jedoch nicht.

5.4.3 Erhebungsmodalitäten

So weit ist die Lage in den beiden Ländern ähnlich. Einen wichtigen Unterschied gibt es bei den Modalitäten der Datenerhebung. In der Schweiz erfolgt diese über den Dienst für die Überwachung des Post- und Fernmeldeverkehrs (Dienst ÜPF).⁷¹ Dieser hat die Funktion einer Drehscheibe zwischen den Behörden und CSP: Die Überwachungsanordnungen sowie die resultierenden Daten werden – gegebenenfalls mit Ermächtigung des Zwangsmassnahmengerichts – über diese Drehscheibe ausgetauscht.

Der *CLOUD Act* hingegen basiert auf der Prämisse, dass die CSP direkt aufgefordert werden und verpflichtet sind, die Daten herauszugeben. Ein solcher Direktzugriff auf die CSP würde aber die folgenden Problempunkte aufwerfen:

- Es wäre systemwidrig, den US-Behörden den Direktzugriff auf CSP zu ermöglichen, während die Schweizer Behörden den Dienst ÜPF zwischenschalten müssen. Es stellt sich die Frage der Gleichbehandlung. Und ein wichtiger Aspekt hierzu ist die Kostenfrage: Die Schweizer Behörden zahlen für die Nutzung des Dienstes ÜPF hohe Gebühren, die beim Direktzugriff nicht – oder nicht so – anfallen würden.
- Dies würde ferner zu einer Erhebung auf zwei Gleisen führen: Die CSP, die unter dem BÜPF Abläufe und Protokolle für die Abfrage durch den Dienst ÜPF eingerichtet haben, müssten parallel dazu US-Behörden auf anderem Weg bedienen.
- Ob die Echtzeit-Überwachung so überhaupt möglich wäre, ist fraglich: Die Überwachung wird i. d. R. durch den CSP auf Anordnung der Strafverfolgungsbehörde und Verfügung des Dienstes ÜPF vorgenommen, manchmal muss sie aber nur vom Anbieter ermöglicht und geduldet werden. Dem Vernehmen nach bedingt die Überwachung umfangreiche technische Vorbereitungen, die von Fall zu Fall stark variieren. Es ist deshalb zweifelhaft, ob dies im bilateralen Verhältnis zwischen einer US-Behörde und einem Schweizer CSP bewerkstelligt werden könnte.
- Die Verfügungen des Dienstes ÜPF sind Verfügungen i. S. v. Artikel 5 des Bundesgesetzes vom 20. Dezember 1968 über das Verwaltungsverfahren (nachfolgend VwVG)⁷². Der betroffene CSP kann dagegen (insbesondere gegen Verfügungen, mit denen eine Überwachung zur Umsetzung einer Überwachungsanordnung angeordnet wird, die von einer Strafverfolgungsbehörde erlassen/übermittelt wurde) in eingeschränktem Rahmen Rechtsmittel ergreifen. Dies könnte *de facto* noch stärker eingeschränkt oder gar ausser Kraft gesetzt werden, wenn der Dienst ÜPF keine Rolle mehr spielt bzw. diese Verfügungen nicht mehr übermittelt.

Denkbar wäre es, den US-Behörden den Zugang ebenfalls über den Dienst ÜPF zu gewähren. Dies würde allerdings eine massive Aufgabenausweitung für den Dienst ÜPF bedeuten. Ausserdem «passt» der *CLOUD Act* nach seinem Wortlaut nicht auf diese Lösung, da er

⁷⁰ Vgl. die Definition in Art. 8 Bst. b BÜPF: «Daten, aus denen hervorgeht, mit wem, wann, wie lange und von wo aus die überwachte Person Verbindung hat oder gehabt hat, sowie die technischen Merkmale der entsprechenden Verbindung».

⁷¹ «Dienst für die Überwachung des Post- und Fernmeldeverkehrs gemäss Artikel 269 der Strafprozessordnung (StPO)», vgl. Art. 3 BÜPF.

⁷² SR 172.021

Bericht zum US Cloud Act

von der Prämisse ausgeht, dass die Daten direkt beim CSP erhoben werden (allerdings könnten evtl. im *Executive Agreement* die nötigen Anpassungen vereinbart werden).

Die Vorteile einer Lösung via Dienst ÜPF lägen aber auf der Hand: Was die Datenerhebung betrifft, wäre insoweit Gleichbehandlung zwischen US- und den schweizerischen Behörden erstellt (u. a. müssten die US-Behörden mit denselben Gebühren belastet werden). Ausserdem hätten die US-Behörden einen *single point of contact*, einen einzigen Ansprechpartner, was im internationalen Verkehr ohnehin von Vorteil ist. Noch weitergedacht, könnte der Dienst ÜPF so die Rolle einer Zentralbehörde für die US-Datenerhebung einnehmen. Damit könnten Bedenken begegnet werden, die im Wegfallen der Aufsichtsfunktion des BJ begründet liegen: Beim direkten Zugriff, wie er im *CLOUD Act* vorgesehen ist, ist nicht klar, wer die in der Rechtshilfe geltenden Ausschlussgründe prüft, wer die Einhaltung des Spezialitätsgrundsatzes überwacht etc. Wie aber der schweizseitige Rechtsschutz funktionieren könnte, ist – wie unten aufgezeigt wird – ebenso noch zu definieren (siehe Ziff. 5.6)

5.5 Schutz der Grundrechte, insbesondere der Daten und des Privatlebens

5.5.1 Die EU-Ebene: Verhältnis zwischen dem *CLOUD Act* und der EU-Datenschutz-Grundverordnung DSGVO

5.5.1.1 Vereinbarkeit des *CLOUD Acts* mit der DSGVO

Die Vereinbarkeit des *CLOUD Acts* und eines allfälligen, gestützt auf dessen Grundsätze abgeschlossenen *Executive Agreements* mit dem Recht der EU, namentlich deren Datenschutz-Grundverordnung⁷³ (DSGVO), die seit 2018 in Kraft ist, ist auch für die Schweiz von Bedeutung. Die DSGVO ist für die Schweiz als Nicht-Mitgliedstaat der EU zwar nicht unmittelbar anwendbar, da es sich nicht um eine Weiterentwicklung des Schengen-Acquis handelt. Ihre Bestimmungen gelten aber für Unternehmen in der Schweiz, die gemäss Artikel 3 DSGVO in den Geltungsbereich der Verordnung fallen. Dies ist vorliegend namentlich dann der Fall, wenn der seine Dienstleistungen erbringende CSP innerhalb der EU niedergelassen ist oder, bei fehlender Niederlassung, wenn eine Datenbearbeitung im Zusammenhang damit steht, betroffenen Personen in der EU Dienstleistungen anzubieten oder deren Verhalten zu beobachten, soweit dies in der EU erfolgt.

Um mit der EU und ihren Mitgliedstaaten ungehindert Personendaten austauschen zu können, muss die Schweiz von der Europäischen Kommission weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau gemäss Artikel 45 DSGVO anerkannt bleiben. Die Beibehaltung des *Angemessenheitsbeschlusses* setzt voraus, dass das schweizerische Recht den datenschutzrechtlichen Anforderungen der Verordnung gleichwertig ist. Die Beurteilung der Kompatibilität des *CLOUD Acts* und des allfälligen Abschlusses eines darauf gründenden *Executive Agreements* mit der DSGVO hat entsprechend Folgen im Hinblick auf den für die Schweiz notwendigen Angemessenheitsbeschluss der EU. Dafür spricht auch, dass die Europäische Kommission in ihrer Beurteilung der Angemessenheit des UK-Datenschutzniveaus mit Blick auf die DSGVO das UK-US-*CLOUD Act* Agreement auf dessen Vereinbarkeit mit dem EU-Datenschutzrecht hin überprüfte.⁷⁴ Nicht geprüft wird im vorliegenden Kontext demgegenüber die Situation mit Blick auf die Richtlinie (EU) 2016/680⁷⁵ zum Datenschutz in

⁷³ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG; ABl. L 119/2016 v. 4. Mai 2016.

⁷⁴ Durchführungsbeschluss der Kommission vom 28. Juni 2021 gemäss der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich: C(2021) 4800 final, Ziff. 153 - 156.

⁷⁵ Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung

Bericht zum US Cloud Act

Strafsachen. Sie ist zwar Schengen-relevant und damit von der Schweiz anzuwenden, hier aber insofern nicht von Bedeutung, als der *CLOUD Act* Datenbekanntgaben von privaten CSP an Strafverfolgungsbehörden und nicht Datenbekanntgaben durch (Strafverfolgungs-)Behörden regelt, welche die (ausschliesslichen) Adressaten der Richtlinie sind. Das UK-US-*CLOUD Act* Agreement scheint schliesslich auch keine Bedeutung für die Beurteilung der Angemessenheit des UK-Datenschutz-niveaus mit Blick auf die Richtlinie (EU) 2016/680 durch die Europäische Kommission gehabt zu haben.⁷⁶

Die Prüfung der massgebenden Rechtsgrundlagen ergibt zusammengefasst, dass Datenbearbeitungen gestützt auf Anordnungen einer US-Strafverfolgungsbehörde im Rahmen des *CLOUD Acts* im Hinblick auf die *Rechtmässigkeit* als problematisch zu beurteilen sind. Dies gilt sowohl für die Aufbewahrung von Personendaten als auch für deren Offenlegung.

Zwar anerkennt neben dem Europäischen Datenschutzausschuss (EDSA) und dem Europäischen Datenschutzbeauftragten (EDSB) auch die Europäische Kommission im Grundsatz, dass gestützt auf die einschlägigen Artikel 6 und insbesondere Artikel 49 DSGVO in ganz bestimmten Ausnahmesituationen eine Datenbearbeitung bzw. die Bekanntgabe von Daten an einen Drittstaat auch dann gerechtfertigt sein kann, wenn dieser Staat weder über einen Angemessenheitsbeschluss der Europäischen Kommission noch über spezifische Garantien (Art. 46 DSGVO) mit Bezug auf den Schutz der Daten verfügt. Dies wäre namentlich der Fall, wenn der CSP die Personendaten *zum Schutz der lebenswichtigen Interessen der betroffenen Person selbst* bekannt geben würde (Art. 6 Abs. 1 Bst. d i. V. m. Art. 49 Abs. 1 Bst. f DSGVO). Nicht ausgeschlossen ist des Weiteren, dass sich eine solche Datenbekanntgabe durch ein in der EU und den Mitgliedstaaten anerkanntes öffentliches Interesse rechtfertigen liesse, sofern beispielsweise konkrete Anzeichen für einen schweren Straftatbestand oder einen terroristischen Anschlag in der EU bestehen würden (Art. 49 Abs. 1 Bst. d DSGVO). Jedoch dürfte dieser Ausnahmetatbestand in der Praxis nur sehr schwer zu erfüllen sein, da die DSGVO solche Bekanntgaben aufgrund der besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen nur unter sehr strikt auszulegenden Voraussetzungen und in absoluten Ausnahmefällen erlaubt.

Auch im Hinblick auf weitere Kernelemente der DSGVO könnten sich Datenbearbeitungen gestützt auf den *CLOUD Act* als heikel erweisen:

Unter dem Gesichtspunkt der Transparenz könnte es problematisch sein, dass die US-Strafverfolgungsbehörden in gewissen Fällen nicht verpflichtet sind, die betroffenen Personen über die Bekanntgabe der Daten zu benachrichtigen und mittels gerichtlicher Verfügung auch den CSP verpflichten können, die betroffene Person nicht über die Bekanntgabe ihrer Daten zu informieren.⁷⁷ Nach europäischem Rechtsverständnis wird die Information der betroffenen Person über jeden behördlichen Zugang zu ihren Daten auch im Bereich der Strafverfolgung

von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates; ABI L 119/89 v. 4.5.2016.

⁷⁶ Durchführungsbeschluss der Kommission vom 28. Juni 2021 gemäss der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich: C(2021) 4801 final. Um der Stellungnahme 15/2021 des Europäischen Datenschutzausschusses zum Angemessenheitsbeschluss von UK nach der Richtlinie (EU) 2016/680 Rechnung zu tragen, welcher insbesondere die im UK-US CLOUD Act Agreement vorgesehenen Abhörungsanordnungen äusserst kritisch beurteilt, hat die Europäische Kommission ihren Beschluss ergänzt. Im Rahmen der Überwachung der künftigen datenschutzrelevanten Entwicklungen im Vereinigten Königreich wird sie besondere Aufmerksamkeit auf den Abschluss von internationalen Abkommen legen, welche Auswirkungen auf das gegenwärtige Datenschutzniveau haben (Rz. 165 des Beschlusses). Selbst wenn jedoch die Richtlinie (EU) 2016/680 in der EU so ausgelegt wird, dass sie zusätzlich zu Datenbekanntgaben auch Datenbearbeitungen durch Strafverfolgungsbehörden umfasst, gilt in der Schweiz ein engeres Verständnis des Geltungsbereichs dieser Richtlinie, welchen wir vorliegend nicht tangiert sehen.

⁷⁷ *CLOUD Act*, § 2703 (b) (1) und § 2705 (b).

Bericht zum US Cloud Act

und -vollstreckung als unverzichtbar erachtet.⁷⁸ Gemäss EuGH muss die betroffene Person spätestens dann über die Weitergabe ihrer Personendaten an ausländische Strafverfolgungsbehörden informiert werden, wenn dies die entsprechenden Ermittlungen nicht mehr beeinträchtigen kann.⁷⁹

Mit Bezug auf die Verhältnismässigkeit kommen der EDSA und der EDSB zum Schluss, dass im *CLOUD Act* diesem Grundsatz im Allgemeinen Rechnung getragen wird.⁸⁰ So kann eine US-Strafverfolgungsbehörde die Offenlegung von Personendaten nur verlangen, wenn ein Gericht die Herausgabe zuvor genehmigt und die Behörde durch eidesstattliche Erklärung dargelegt hat, dass ein hinreichender Verdacht besteht, dass ein bestimmtes Verbrechen stattgefunden hat oder stattfindet und die herausverlangten Informationen Beweise für dieses bestimmte Verbrechen enthalten.⁸¹ Die Herausgabeanordnung muss die geforderten Personendaten zudem genau beschreiben, da sogenannte *Fishing expeditions*, um zu sehen, ob Beweise vorhanden sind, nicht zulässig sind.⁸² Die europäischen Datenschutzbehörden stellen aber auch fest, dass im Falle anderer Formen von Anfragen keine entsprechenden richterlichen Kontrollen verlangt werden.⁸³ Hier müsste im Einzelfall geprüft werden, ob eine Datenbearbeitung verhältnismässig wäre oder nicht.

Im Gegensatz zur DSGVO, welche die Personendaten aller natürlichen Personen gleichermaßen schützt, ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsortes, unterscheidet der *CLOUD Act* zwischen Daten von «US-Personen» und von anderen Personen. Namentlich kann im Falle des Vorliegens eines *Executive Agreements* ein CSP nur dann die gerichtliche Kontrolle einer Anordnung einer US-Strafverfolgungsbehörde im Falle kollidierender rechtlicher Verpflichtungen verlangen, wenn es sich nicht um Personendaten von US-Personen handelt.⁸⁴ Gemäss EDSB ist hingegen jegliche Ungleichbehandlung aus datenschutzrechtlicher Sicht aufgrund der Staatsangehörigkeit oder der Ansässigkeit der betroffenen Person mit der DSGVO unvereinbar.⁸⁵

Der *CLOUD Act* sieht keine datenschutzrechtlichen Garantien für die betroffenen Personen vor, etwa in Form eines Zugangs- oder Auskunftsrechts hinsichtlich ihrer Daten. Vielmehr erlaubt er, in gewissen Fällen ganz von einer Information der betroffenen Personen über eine Datenbekanntgabe an eine US-Strafverfolgungsbehörde abzusehen.⁸⁶ Dies widerspricht grundsätzlich Artikel 8 Absatz 2 der europäischen Grundrechtscharta⁸⁷, wo in Bezug auf die Bearbeitung von Personendaten explizit das Recht auf Auskunft und das Recht auf Berichtigung garantiert wird.

Der *CLOUD Act* sieht keine Möglichkeit für die von einer Herausgabeanordnung betroffene Person vor, sich gegen die Bekanntgabe ihrer Personendaten zur Wehr zu setzen. Eine begrenzte Abwehrmöglichkeit ist in Fällen einer Rechtskollision nur für den CSP vorgesehen, und nur unter der Voraussetzung, dass ein *Executive Agreement* zwischen der USA und

⁷⁸ Siehe unter anderem EuGH, Gutachten 1/15 EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Rn. 220 und Stellungnahme 23/2018 des EDSA, S. 19.

⁷⁹ EuGH, Gutachten 1/15 EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Rn. 220.

⁸⁰ EDSA/EDSB, Initial legal assessment, S. 2.

⁸¹ DOJ, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the *CLOUD Act*", S. 8.

⁸² Idem, S. 8.

⁸³ EDSA/EDSB, Initial legal assessment, S. 2.

⁸⁴ *CLOUD Act* § 2703.

⁸⁵ Stellungnahme 2/2019 des EDSB, Ziff. 50.

⁸⁶ *CLOUD Act* § 2703 (b) (1) und § 2705 (b).

⁸⁷ Charta der Grundrechte der Europäischen Union, ABl. 2000/C 364/01 vom 18.12.2000.

dem entsprechenden Staat abgeschlossen wurde.⁸⁸ Der betroffenen Person steht gegen eine solche Anordnung hingegen weder eine Beschwerde an eine unabhängige Aufsichtsbehörde zur Verfügung, noch ein gerichtlicher Rechtsbehelf gegen die Bekanntgabe. Das Fehlen eines Rechts auf einen wirksamen gerichtlichen Rechtsbehelf steht im Widerspruch zu dem in Artikel 47 der europäischen Grundrechtscharta garantierten Recht auf wirksamen gerichtlichen Rechtsschutz. Ausserdem betont der EuGH die Wichtigkeit, dass eine betroffene Person einen administrativen Rechtsbehelf bei einer unabhängigen Kontrollstelle einlegen kann.⁸⁹

Als wesentliche Garantie des Datenschutzes schreibt Artikel 8 Absatz 3 der europäischen Grundrechtscharta die Kontrolle durch eine unabhängige Stelle vor. Der EDSB betont in dieser Hinsicht, dass auch die zuständigen Behörden des Staates, in deren Regelungshoheit sich die angefragten Personendaten befinden, in die Verfahren um Bekanntgabe elektronischer Beweismittel mit einbezogen werden sollen, damit ein wirksamer Schutz der Grundrechte garantiert werden kann.⁹⁰ Entsprechend sollten auch die zuständigen Datenschutzbehörden bei direkten Anordnungen an die Dienstleister benachrichtigt werden, um eine Kontrolle zu ermöglichen.⁹¹ Dass CSP Personendaten an eine US-Strafverfolgungsbehörde bekannt geben, ohne die eigenen zuständigen Behörden zu benachrichtigen, könnte sich vor diesem Hintergrund als problematisch erweisen.

5.5.1.2 Fazit: Risiko des Abschlusses eines *Executive Agreements* mit den USA im Hinblick auf den Angemessenheitsbeschluss der Schweiz

Der in Ziff. 5.5.1.1 erwähnte *Angemessenheitsbeschluss* wird von der Kommission regelmässig, nämlich mindestens alle vier Jahre, überprüft (Art. 97 DSGVO). Zu den wesentlichen Aspekten, die bei der Überprüfung berücksichtigt werden, gehören die Datenschutzvorschriften, die Vorschriften betreffend die Weiterübermittlung personenbezogener Daten an ein anderes Drittland sowie der Abschluss internationaler Übereinkommen in Bezug auf den Schutz von Personendaten. Der EuGH hat im Urteil *Schrems II* im Zusammenhang mit dem Zugriff von Behörden auf Personendaten, welche im Empfängerstaat zu Zwecken der nationalen Sicherheit weitergegeben wurden, präzisiert, dass die Kommission bei ihrem Entscheid das im Empfängerstaat geltende innerstaatliche Recht berücksichtigen muss. Das entscheidende Kriterium für die Angemessenheit ist, ob die Regelung, die den Zugriff der Behörden im Empfängerstaat zum Zweck der nationalen Sicherheit erlaubt, auch klare Bestimmungen zur Beschränkung des Zugriffs enthält, also klar festhält, unter welchen Voraussetzungen und Umständen dieser Zugriff erlaubt ist. Er muss auf das absolut Nötigste beschränkt sein.⁹² Darüber hinaus muss die einschlägige Regelung im Empfängerstaat wirksame und durchsetzbare Rechte zum Schutz der betroffenen Person vor allfälligen Missbräuchen vorsehen.⁹³

Der Schweiz wurde im Jahr 2000 von der EU attestiert, dass sie über ein angemessenes Datenschutzniveau verfügt. Dieser Angemessenheitsbeschluss gilt vorerst auch unter der seit dem 25. Mai 2018 anwendbaren DSGVO weiter. Im Frühjahr 2019 hat die Europäische Kommission mit der erneuten Evaluierung der Schweiz begonnen. Dabei führt sie die Überprüfung auf der Grundlage des geltenden schweizerischen Rechts durch, hat sich aber bereit gezeigt, die anlässlich der Revision des Datenschutzgesetzes (DSG) einzuführenden Stärkungen

⁸⁸ Siehe hierzu vorne Ziffer 3.2.2.

⁸⁹ Entscheid des EuGH, *Maximilian Schrems vs. Data Protection Commissioner*, C-362-14, Rn. 56 – 58.

⁹⁰ Stellungnahme 2/2019 des EDSB, Ziff. 28. Im Kontext mit den Europäischen Herausgabe- und Sicherungsanordnungen für Elektronische Beweismittel in Strafsachen, siehe auch Stellungnahme 23/2018 des EDSA, S. 16.

⁹¹ Siehe Stellungnahme 23/2018 des EDSA, S. 8.

⁹² EuGH, *Schrems II*, E. 175-176.

⁹³ EuGH, *Schrems II*, E. 177-178.

Bericht zum US Cloud Act

des Datenschutzes zu berücksichtigen, sofern die Totalrevision des DSG (nDSG) zeitnah abgeschlossen wird. Da das nDSG am 25. September 2020 von den Eidgenössischen Räten genehmigt wurde (vgl. unten 5.5.2.1.) und das Inkrafttreten des neuen Gesetzes sowie der dazugehörigen Verordnungen für die zweite Hälfte 2022 geplant ist, sollte dies gegeben sein.

In ihrem Beschluss über die Angemessenheit des UK Datenschutzniveaus gemäss DSGVO – welcher von der Europäischen Kommission zusammen mit dem Beschluss über die Angemessenheit von UK nach der Richtlinie (EU) 2016/680 am 28. Juni 2021 verabschiedet wurde – beurteilte die Kommission auch das UK-US *CLOUD Act* Agreement.⁹⁴ Dies zeigt, dass auch der Inhalt eines *Executive Agreements* zwischen der Schweiz und den USA im Hinblick auf eine erneute Beurteilung der Angemessenheit des schweizerischen Datenschutzniveaus berücksichtigt würde.

Im Beschluss mit Blick auf UK hält die Europäische Kommission fest, dass beim Inkrafttreten des UK-US *CLOUD Act* Agreements Daten, welche aus der EU an CSP in UK übertragen werden, Gegenstand von Herausgabeanordnungen von US-Strafverfolgungsbehörden sein könnten. Eine Bewertung der Bedingungen und Garantien, unter denen solche Herausgabeanordnungen ausgeführt werden, ist deshalb im Hinblick auf die Entscheidung der Angemessenheit des UK Datenschutzniveaus relevant. Zwar beurteilt die Kommission das Abkommen im Hinblick auf die Anforderungen der DSGVO nicht per se als unangemessen. Einerseits hebt die Europäische Kommission hervor, dass sie selbst über ein Mandat der Mitgliedstaaten verfügt, in diesem Bereich Verhandlungen mit den USA zu führen und deshalb kein «*double standard*» hinsichtlich eines entsprechenden Abkommens zwischen UK und USA geschaffen werden dürfe. Andererseits bewertet die Kommission insbesondere die im Abkommen festgelegten strengen Anforderungen an Herausgabeanordnungen und an Echtzeit-Überwachungen als positiv, sowie dass darin durch einen Verweis auf das Rahmenabkommen zwischen der EU und den USA⁹⁵ alle in jenem festgelegten Garantien und Rechte sinngemäss Anwendung finden.⁹⁶ Die Kommission hält zudem fest, dass die britischen Behörden ihr gegenüber bestätigten, dass das Abkommen erst in Kraft treten soll, wenn die Einhaltung dieser Datenschutzstandards für alle im Rahmen dieses Abkommens übermittelten Daten sichergestellt sei.

Wesentlich skeptischer zeigen sich in diesem Hinblick der EDSA⁹⁷ und das Europäische Parlament⁹⁸. Diese bezweifeln insbesondere, ob mit einem blossen Verweis auf das EU-US Rahmenabkommen die darin garantierten datenschutzrechtlichen Ansprüche durch betroffene Personen nach britischem Recht wirksam und einklagbar wären sowie ob die darin vorgesehenen Schutzmassnahmen auf alle Herausgabeanordnungen der US-Strafverfolgungsbehörden Anwendung fänden – oder ob nicht doch amerikanisches Recht vorgehe. Die Kommission hält diesen Befürchtungen entgegen, dass der Angemessenheitsbeschluss eine kontinuierliche Überwachung der relevanten Entwicklungen in diesem Bezug vorsehe. Die Kommission werde dabei ein besonderes Augenmerk auf die Anwendung und die Umsetzung der Garantien des Rahmenabkommens im Rahmen von entsprechenden Datenübermittlungen richten und die notwendigen Konsequenzen ziehen, sofern es Anzeichen dafür gebe, dass

⁹⁴ Rz. 153 – 156 des Angemessenheitsbeschlusses von UK nach der DSGVO.

⁹⁵ Siehe FN 41

⁹⁶ Artikel 9 Absatz 1 des UK-US *CLOUD Act* Agreements hält entsprechend fest, dass ein diesem Rahmenabkommen gleichwertiger Schutz «auf alle Personendaten Anwendung findet, welche bei der Ausführung von Anordnungen, die gestützt auf das Abkommen ergehen, erhoben werden.»

⁹⁷ Stellungnahme des EDSA 14/2021 vom 13. April 2021 zum Entwurf des Durchführungsbeschlusses der Europäischen Kommission gemäss der Verordnung (EU) 2016/679 über die Angemessenheit des Schutzes personenbezogener Daten im Vereinigten Königreich, Rz. 88 ff.

⁹⁸ Entschliessung des Europäischen Parlaments vom 21. Mai 2021 zu der Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich (2021/2594(RSP)), Ziff. 25.

Bericht zum US Cloud Act

ein gleichwertiges Schutzniveau nicht mehr gewährleistet sei. Als wesentliche Massnahme in dieser Hinsicht betont die Europäische Kommission auch die in Artikel 4 des Angemessenheitsbeschlusses festgelegte «*sunset clause*», gemäss welcher die Geltungsdauer des Angemessenheitsbeschlusses des UK Datenschutzniveaus nach vier Jahren automatisch endet, sofern keine zusätzliche Vereinbarung getroffen wird.

Selbst wenn nach Ansicht der Europäischen Kommission das UK-US-*CLOUD Act* Agreement mit den europäischen Datenschutzstandards vereinbar ist, ist die Ausgangslage mit Blick auf die Schweiz eine andere. So setzt UK, mit Ausnahme des Bereiches der Einwanderungskontrolle,⁹⁹ im Unterschied zur Schweiz die DSGVO zumindest momentan noch vollständig um. Zudem stellen der Verweis auf das Rahmenabkommen zwischen der EU und den USA sowie die entsprechende Versicherung der britischen Behörden, das Abkommen nur bei Gewährleistung der entsprechenden Garantien in Kraft treten zu lassen, nach Ansicht der Kommission sicher, dass die Personendaten, welche gestützt auf das UK-US *CLOUD Act* Abkommen übermittelt würden, weiterhin dem Schutz eines EU-Rechtsinstrumentes unterstehen.

In diesem Hinblick scheinen die Möglichkeiten für die Schweiz eingeschränkter. Aufgrund des engen und aus datenschutzrechtlicher Sicht problematischen Rahmens des *CLOUD Acts* ist nicht davon auszugehen, dass die Schweiz mit dem Abschluss eines *Executive Agreements* den oben beschriebenen datenschutzrechtlichen Anforderungen genügen könnte. So verfolgt auch die Kommission mit ihren eigenen Verhandlungen mit den USA das Ziel eines *umfassenden Abkommens*, das den Austausch elektronischer Beweismittel regelt und damit weitergeht als ein *Executive Agreement*, wie es im *CLOUD Act* vorgesehen ist. Ein umfassender Rechtsschutz, wie er vom europäischen Datenschutzrecht verlangt und nach Ansicht der Kommission im Fall von UK gewährleistet ist, könnte für die Schweiz deshalb wohl nur durch den Abschluss eines *umfassenden* Abkommens mit den USA erreicht werden. Dieses müsste den Austausch elektronischer Beweismittel regeln und *gleichzeitig* ein hohes, den europäischen und nationalen Standards entsprechendes Datenschutzniveau vorsehen. Schliesslich müsste im Einklang mit den Forderungen des EDSA sichergestellt werden, dass ein solches Abkommen im Fall des Datenaustauschs zwischen CSP und Strafverfolgungsbehörden *dem US-Recht vorginge*.

Überdies ist anzunehmen, dass die Europäische Kommission den zum UK-US *CLOUD Act* Agreement geäusserten Bedenken des EDSA und des Europäischen Parlaments im Hinblick auf künftige Angemessenheitsbeschlüsse mehr Gewicht einräumen wird als im Fall von UK. Hier schien der Zeitdruck ein wesentlicher Faktor zu sein, nach Ende der Übergangsfrist eine Rechtsgrundlage für Datentransfers aus der EU nach UK zu haben. Dieser Faktor scheint die Kommission dazu bewogen zu haben, trotz dem Widerstand des Parlaments und des EDSA nicht von ihrem Vorhaben abzuweichen, die Angemessenheitsbeschlüsse mit Blick auf UK bis Ende Juni 2021 zu verabschieden. Wie bereits erwähnt, wurden die Beschlüsse am 28. Juni verabschiedet und sind auf 2025 befristet.

In ihren Angemessenheitsbeschlüssen mit Blick auf UK betont die Europäische Kommission, dass sie sich bei ihren Beurteilungen wesentlich vom Urteil des EuGH zur Rechtssache *Schrems II* vom 16. Juli 2020 leiten lasse. Dies spricht ebenfalls für ein bedachtsames Vorgehen der Schweiz, hat der Gerichtshof darin doch befunden, dass die Europäische Kommission beim Entscheid über die Angemessenheit der Bekanntgabe von Daten an die USA im

⁹⁹ Aufgrund des Urteils des UK *Court of Appeal* vom 26. Mai 2021, mit welchem die in UK vorgesehenen Ausnahmeregelungen von datenschutzrechtlichen Ansprüchen im Bereich der Einwanderungskontrolle als mit der DSGVO unvereinbar beurteilt werden, schliesst die Europäische Kommission diesen Bereich vom Angemessenheitsbeschluss nach der DSGVO vorläufig aus. Sobald feststeht, ob und wie UK diese Mängel beheben wird, wird die Kommission einen Wiedereinbezug prüfen und den Beschluss gegebenenfalls entsprechend anpassen (Rz. 6 des Angemessenheitsbeschlusses von UK nach der DSGVO).

Rahmen des *Privacy-Shield-Abkommens* nicht berücksichtigt hat, dass die Bestimmungen zu den staatlichen Überwachungsprogrammen im amerikanischen Recht keine hinreichenden Garantien zur Erfüllung der Anforderungen der DSGVO bezüglich Datenschutz und keinen genügenden Rechtsschutz für die betroffenen «nicht US Personen» bieten.¹⁰⁰ Daraus kann geschlossen werden, dass die Europäische Kommission im Rahmen künftiger Angemessenheitsbeschlüsse bei der Beurteilung der Garantien, die völkerrechtliche Verträge zur Behebung solcher grösserer Datenschutzlücken bieten, noch strenger sein wird. Überdies zeigen die derzeit vorgenommenen Angleichungen von weiteren Rechtsakten auf dem Gebiet der Strafverfolgung und -vollstreckung an die Richtlinie (EU) 2016/680,¹⁰¹ dass die EU künftig die Voraussetzungen für den Datenaustausch in diesen Bereichen noch strenger handhaben wird.

5.5.2 Rechtmässigkeit der Bearbeitung und Bekanntgabe von Daten gestützt auf eine Herausgabeeanordnung auf der Grundlage des *CLOUD Acts* nach Schweizer Recht

5.5.2.1 Der vorliegend relevante datenschutzrechtliche Rahmen in der Schweiz

Auf Bundesebene ist der Datenschutz gegenwärtig primär im Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)¹⁰² geregelt. Gegenstand des DSG ist die Bearbeitung von Daten durch Bundesorgane wie auch durch Privatpersonen. Zahlreiche bereichsspezifische Datenschutznormen regeln zudem in Spezialgesetzen die Bearbeitung von Daten durch Bundesorgane. Für die Bearbeitung von Daten durch Bundesorgane und Private finden zudem die Verordnung vom 14. Juni 1993¹⁰³ zum Bundesgesetz über den Datenschutz (VDSG) sowie die Verordnung vom 28. September 2007¹⁰⁴ über die Datenschutzzertifizierungen Anwendung. Die Bearbeitung von Daten durch kantonale oder kommunale Organe wird in den kantonalen Datenschutzgesetzen geregelt.

Am 25. September 2020 hat das Parlament die Totalrevision des DSG verabschiedet (nDSG).¹⁰⁵ Zurzeit läuft die Vernehmlassung zur revidierten VDSG. Das Inkrafttreten der revidierten Datenschutzgesetzgebung ist nach derzeitigem Stand für die zweite Hälfte 2022 geplant. Mit der Totalrevision des Datenschutzrechts wird der schweizerische Datenschutz im Einklang mit dem europäischen Datenschutzniveau wesentlich gestärkt.

Für die Frage der Vereinbarkeit der Bearbeitung von Daten gestützt auf Herausgabeeanordnung mit dem schweizerischen Datenschutzrecht sind das geltende DSG, die VDSG sowie die relevanten Bestimmungen des totalrevidierten DSG (inkl. VDSG) massgebend. Im vorliegenden Zusammenhang nicht speziell berücksichtigt werden müssen demgegenüber aufgrund seines Geltungsbereichs das Bundesgesetz vom 28. September 2018¹⁰⁶ über den Datenschutz in Anwendung des Schengen-Besitzstands in Strafsachen (SDSG) wie auch die von der Schweiz unterzeichnete, revidierte Datenschutzkonvention 108+ des Europarates. Letztere ist inhaltlich der Richtlinie (EU) 2016/680 und der DSGVO sehr ähnlich; die darin enthaltenen Grundsätze wurden im Rahmen der DSG-Revision berücksichtigt.

¹⁰⁰ EuGH, *Schrems II*, E. 175-178.

¹⁰¹ Siehe «Communication from the Commission to the European Parliament and the Council; Way forward on aligning the former third pillar acquis with data protection rules», einsehbar auf https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v7.pdf (Stand 07.06.2021).

¹⁰² SR 235.1

¹⁰³ SR 235.11

¹⁰⁴ SR 235.13

¹⁰⁵ BBl 2020 7639

¹⁰⁶ SR 235.3

5.5.2.2 Problematische Aspekte im Hinblick auf die Grundsätze des schweizerischen Datenschutzrechts

Das schweizerische Datenschutzrecht geht von einem anderen Ansatz aus als das Verständnis der DSGVO, wonach die Bearbeitung von Daten durch Privatpersonen grundsätzlich widerrechtlich ist, ausser sie lasse sich auf einen Rechtfertigungsgrund stützen. Datenbearbeitungen durch Private sind in der Schweiz grundsätzlich erlaubt, soweit sie nicht Persönlichkeitsverletzend sind. Eine Persönlichkeitsverletzung liegt insbesondere vor, wenn eine Datenbearbeitung gegen die allgemeinen Grundsätze in Artikel 4 DSG/Artikel 6 nDSG (insb. Rechtmässigkeit, Bearbeitung nach Treu und Glauben, Verhältnismässigkeit, Zweckgebundenheit und Erkennbarkeit der Datenbearbeitung für die betroffene Person) verstösst oder die Anforderungen an die Datenrichtigkeit (Art. 5 DSG/Art. 6 Abs. 5 nDSG) und an die Datensicherheit (Art. 7 DSG/Art. 8 nDSG) nicht erfüllt (Art. 12 Abs. 2 Bst. a DSG bzw. Art. 30 Abs. 2 Bst. a nDSG).¹⁰⁷ Diese Grundsätze finden sich generell unverändert im revidierten Recht wieder. Kumulativ zu den datenschutzrechtlichen Grundsätzen müssen Datenbekanntgaben ins Ausland zudem die Anforderungen von Artikel 6 DSG erfüllen¹⁰⁸, welche grundsätzlich auch im revidierten Recht übernommen wurden (Art. 16 f. nDSG).

Im Hinblick auf die datenschutzrechtlichen Grundsätze scheinen Datenbearbeitungen gestützt auf den *CLOUD Act* in verschiedener Hinsicht als problematisch. So verlangt der Grundsatz von Treu und Glauben, dass die allgemeinen Regeln mit Bezug auf die Datenbearbeitung angewendet werden. Dies gilt auch dann, wenn Vorschriften und Garantien mit Bezug auf den Datenschutz unvollständig oder nicht konkret sind. Davon betroffen ist insbesondere die Frage der Transparenz einer Datenbearbeitung. Vor diesem Hintergrund könnten Datenbearbeitungen, welche gestützt auf Herausgabeanordnungen vorgenommen werden, in verschiedener Hinsicht problematisch sein. Die Bekanntgabe von Daten, die nicht gestützt auf ein Rechtshilfeersuchen erfolgt, kann als Verstoss gegen Treu und Glauben angesehen werden. Das Gleiche lässt sich auch in Bezug auf Datenbearbeitungen sagen, die heimlich erfolgen oder mit denen die betroffene Person nicht rechnen muss.¹⁰⁹ Als problematisch könnte sich zudem die Bestimmung im *CLOUD Act* erweisen, welche die Information der betroffenen Person vor dem vorstehenden Zugriff der Behörden auf die Daten gänzlich untersagt.

Gemäss dem Grundsatz der Verhältnismässigkeit dürfen nur Daten bearbeitet werden, die für den Zweck der Bearbeitung geeignet und notwendig sind. Zwischen dem Zweck und den verwendeten Mitteln muss ein angemessenes Verhältnis bestehen, und die Rechte der betroffenen Personen sind soweit wie möglich zu wahren.¹¹⁰ Der Grundsatz gilt auch für Privatpersonen, die Daten bearbeiten. Dabei ist immer die Interessenlage des Datenbearbeiters und jene der betroffenen Person zu berücksichtigen. Insofern, als der *CLOUD Act* im Rahmen von Herausgabeanordnungen eine gerichtliche Überprüfung vorsieht (vgl. Ziff. 3.2.1), kann prinzipiell davon ausgegangen werden, dass dem Grundsatz der Verhältnismässigkeit Rechnung getragen wird. Der Umstand, dass bei anderen Formen von Anfragen keine derartige Kontrolle verlangt wird, könnte sich mit Bezug auf die Verhältnismässigkeit hingegen als problematisch erweisen. Zudem ist unter dem Aspekt der Notwendigkeit zu prüfen, ob der Weg über die klassische Rechtshilfe nicht zum gleichen Ziel führen würde und damit als «mildere»

¹⁰⁷ BRUNO BAERISWYL in: BAERISWYL BRUNO (Hrsg.), Stämpflis Handkommentar zum Datenschutzgesetz (SHK DSG), Bern 2015, Vorbemerkungen zu Art. 4 – 11a, Rz. 3.

¹⁰⁸ MAURER-LAMBROU/STEINER in BSK DSG und BGÖ, Art. 6 DSG, Rz. 11a.

¹⁰⁹ Botschaft DSG, BBl 1988 II 413 (449).

¹¹⁰ Botschaft DSG, BBl 1988 II 413 (450).

Bericht zum US Cloud Act

Massnahme, die einen weniger einschneidenden Eingriff in die Persönlichkeitsrechte der betroffenen Person bedeuten würde, zu bevorzugen wäre.

Jede Datenbearbeitung darf nur zu einem bestimmten Zweck erfolgen, der für die betroffene Person zudem erkennbar sein muss. Wenn Private Personendaten bearbeiten, ergibt sich der Zweck dieser Datenbearbeitung primär aus den Angaben, welche der betroffenen Person bei der Erhebung ihrer Daten mitgeteilt werden oder die aus den Umständen ersichtlich sind. Es muss für die betroffene Person nachvollziehbar sein, was mit ihren Daten geschieht. Eine Weiterbearbeitung der Personendaten zu einem anderen Zweck, welcher für sie berechtigterweise als unerwartet und nicht erkennbar angesehen werden kann, würde ihr Recht auf Privatsphäre und auf informationelle Selbstbestimmung verletzen, sofern diese Zweckänderung beispielsweise nicht durch ihre Einwilligung gerechtfertigt wäre. Werden Personendaten gestützt auf Sicherungs- und Herausgabeanordnungen nach dem *CLOUD Act* aufbewahrt oder an US-Strafverfolgungsbehörden bekannt gegeben, stellt dies eine Zweckänderung im Hinblick auf den ursprünglich durch die CSP im Rahmen ihrer vertraglichen Dienstleistung bearbeiteten Personendaten dar. Das Gesetz verlangt in diesem Fall einen entsprechenden Rechtfertigungsgrund für die Zweckänderung und eine Information der betroffenen Personen.

Der Grundsatz der Erkennbarkeit verlangt, dass für die betroffene Person die Beschaffung ihrer Personendaten und insbesondere der Zweck ihrer Bearbeitung erkennbar sein müssen. Dieser Grundsatz ist die Voraussetzung für das Recht auf informationelle Selbstbestimmung und für die Wahrnehmung der datenschutzrechtlichen Ansprüche. Für die Verantwortlichen ergibt sich aus diesem Grundsatz eine Informationspflicht gegenüber der betroffenen Person, sofern für sie eine Datenbearbeitung nicht offensichtlich erkennbar ist.¹¹¹ Auch unter diesem Aspekt erweisen sich Datenbearbeitungen, die gestützt auf Herausgabeanordnungen durch US-Behörden vorgenommen werden, als problematisch, da sie gestützt auf ausländisches Recht erfolgen. Zudem müsste auch geprüft werden, ob der Umstand, dass eine US-Strafverfolgungsbehörde einem CSP mittels gerichtlicher Verfügung untersagen kann, die betroffene Person über die Bekanntgabe ihrer Daten zu informieren, mit dem Grundsatz der Transparenz vereinbar wäre oder sich gegebenenfalls rechtfertigen liesse. Eine Information muss aber spätestens dann erfolgen, sobald dies allfällige Ermittlungen nicht mehr beeinträchtigen kann.

5.5.2.3 Rechtfertigungsgründe für private Personen bei Verletzungen der Persönlichkeit gemäss Artikel 13 DSG/Artikel 27 nDSG

Mögliche Rechtfertigungsgründe, damit eine Datenbearbeitung nicht als widerrechtliche Persönlichkeitsverletzung gilt, sind die Einwilligung der betroffenen Person, ein überwiegendes privates oder öffentliches Interesse oder eine durch Gesetz gerechtfertigte Datenbearbeitung. Gemäss Rechtsprechung des Bundesgerichts lässt sich eine Verletzung der datenschutzrechtlichen Grundsätze von Artikel 4, Artikel 5 Absatz 1 und Artikel 7 Abs. 1 DSG (bzw. Art. 6 und 8 nDSG) dabei aber nur mit grosser Zurückhaltung rechtfertigen.¹¹²

Eine Persönlichkeitsverletzung kann dadurch gerechtfertigt sein, dass die betroffene Person in die Datenbearbeitung einwilligt. Damit die Einwilligung rechtsgültig ist, muss die betroffene Person angemessen über die Datenbearbeitung informiert worden sein. Aufgrund der Informationen muss es ihr möglich sein abzuschätzen, welche Risiken für ihre Persönlichkeitsrechte bestehen. Eine angemessene Information sollte deshalb besonders auch die spezifi-

¹¹¹ BAERISWYL, SHK DSG, Art. 4, Rz. 47 - 50.

¹¹² BGE 136 II 508, Erw. 5.2.4.

sche Risikosituation der Bekanntgabe ins Ausland umfassen und das Fehlen angemessener Datenschutzbestimmungen thematisieren. Die Einwilligung muss zudem freiwillig sein, d.h. dass die betroffene Person muss sich ohne Druck für oder gegen die Datenbearbeitung entscheiden können.¹¹³ In der Literatur wird vertreten, dass eine Einwilligung zudem nur dann freiwillig sein kann, wenn der Person eine mit nicht unzumutbaren Nachteilen behaftete Handlungsalternative zur Verfügung steht.¹¹⁴

Im vorliegenden Kontext ist als problematisch anzusehen, dass bei Datenbearbeitungen gestützt auf Herausgabeanordnungen der Konnex zu der vom CSP für den Kunden zu erbringenden Dienstleistung und der dafür notwendigen Datenbearbeitung fehlt. Der Kunde müsste also diesem für die Dienstleistungserbringung nicht notwendigen Zweck zustimmen, um die Dienstleistung beanspruchen zu können. Wird ein Vertrag von der Einwilligung in eine Datenbearbeitung abhängig gemacht, die für die Vertragserfüllung nicht nötig ist, so wird im EU Recht grundsätzlich davon ausgegangen, dass die Einwilligung nicht freiwillig erfolgt. Bei Datenbearbeitungen im Rahmen der Strafverfolgung und -vollstreckung kann zudem grundsätzlich davon ausgegangen werden kann, dass der betroffenen Person keine echte Wahlfreiheit zukommt. Dies deutet zumindest darauf hin, dass damit die Anforderungen an die rechtsgültige Einwilligung im Zusammenhang mit dem *CLOUD Act* nicht gegeben sein dürften, und ein CSP könnte sich nicht auf die Einwilligung der betroffenen Person als Rechtfertigungsgrund für Datenbearbeitungen und -bekanntgaben gestützt auf Herausgabeanordnungen berufen.

Auch private Verantwortliche können sich auf ein überwiegendes privates oder öffentliches Interesse berufen, um eine persönlichkeitsverletzende Datenbearbeitung zu rechtfertigen. Massgebend ist jedoch, dass im Rahmen einer Interessenabwägung die betroffenen Interessen gegeneinander abgewogen werden und im Ergebnis das private oder öffentliche Interesse höher zu gewichten ist als das Interesse der von der Persönlichkeitsverletzung betroffenen Person. Eine – nicht abschliessende – Aufzählung von möglichen überwiegenden Interessen des Verantwortlichen findet sich in Artikel 13 Absatz 2 DSG respektive in Artikel 31 Absatz 2 nDSG.

Das *Eigeninteresse* des Verantwortlichen kann – neben allfälligen Interessen von Drittpersonen oder ausnahmsweise auch dem Interesse der betroffenen Person selbst – eine Datenbearbeitung rechtfertigen.¹¹⁵ Im Kontext von Datenbearbeitungen gestützt auf Herausgabeanordnungen wäre eine Rechtfertigung im Eigeninteresse des CSP zu prüfen, falls er bei einer Nichtbefolgung der Anordnung mit Sanktionen nach US-Recht zu rechnen hätte. So hat die Europäische Kommission in ihrem Amicus-Curiae-Schreiben zum Microsoft-Fall vor dem Obersten Gerichtshof der USA für diesen Fall ein berechtigtes Interesse des CSP als möglich erachtet. Aber auch im nationalen Kontext dürfte eine Aufbewahrung oder Bekanntgabe von Daten nur dann als rechtmässig erachtet werden, wenn die Interessen der in ihrem Persönlichkeitsrecht verletzten betroffenen Person nicht überwiegen. Es ist jedoch nicht davon auszugehen, dass bei einer Interessenabwägung ein allfälliges Interesse des CSP, nicht sanktioniert zu werden, die Interessen der in ihrem Persönlichkeitsrecht verletzten Person überwiegen würde. So ist grundsätzlich anerkannt, dass das Interesse einer Person am Schutz ihrer Persönlichkeit und am Schutz der Privatsphäre und der informationellen Selbstbestimmung

¹¹³ BAERISWYL, SHK DSG, art. 4, Rz. 65.

¹¹⁴ Siehe RAMPINI in BSK DSG, Art. 13, Rz. 6.

¹¹⁵ WERMELINGER, A., «Art. 13», in Baeriswyl, B. (Hrsg.), *Datenschutzgesetz – Stämpfli Handkommentar*, Bern: Stämpfli 2015, Rz. 11.

Bericht zum US Cloud Act

bereits *an sich* ein gewichtiges Interesse darstellt.¹¹⁶ Bei der Interessenabwägung dürfte so- dann auch hier wesentlich ins Gewicht fallen, dass die USA grundsätzlich weniger starke da- tenschutz- und verfahrensrechtliche Garantien gewähren.

Als Beispiele für *öffentliche* Interessen, die vom privaten Verantwortlichen geltend gemacht werden können, werden in der Literatur die Sicherheit oder der Kampf gegen Geldwäscherei genannt.¹¹⁷ Mit überwiegendem öffentlichen Interesse ist dabei das öffentliche Interesse aus Sicht der Schweiz gemeint. Dieses beschränkt sich nicht auf rein inländische Interessen, son- dern kann auch in der Unterstützung von Anliegen eines ausländischen Staats (beispiels- weise bei der Bekämpfung der Geldwäscherei) liegen oder wenn ein Anliegen eines ausländi- schen Staates eine Reflexwirkung auf die Schweiz zeitigt und damit indirekt auch im öffentli- chen Interesse der Schweiz liegt.¹¹⁸ Ein ausländisches Anliegen beispielsweise im Bereich der Terrorismusbekämpfung könnte demnach ein berechtigtes öffentliches Interesse aus Sicht der Schweiz darstellen.¹¹⁹ Hier scheint die Schweiz weniger restriktiv zu sein als die EU mit der DSGVO, nach welcher ein öffentliches Interesse nur dann vorliegen kann, wenn dies- ses im Unionsrecht oder im Recht eines Mitgliedstaates anerkannt ist.

Sofern das konkret mit einer Herausgabeanordnung verfolgte schwere Verbrechen (*serious crimes*) als im öffentlichen Interesse liegend anerkannt würde und die Bekanntgabe dafür un- erlässlich wäre, könnte sich ein CSP, der in dieser Hinsicht Personendaten bearbeitet, auf diesen Rechtfertigungsgrund berufen. Allerdings muss dieses öffentliche Interesse das Inte- resse der in ihrer Persönlichkeit verletzten betroffenen Person überwiegen. Da Datenbearbei- tungen gestützt auf Anordnungen von US-Strafverfolgungsbehörden jedoch grundsätzlich als nicht vereinbar mit den hier geltenden datenschutzrechtlichen Grundsätzen anzusehen sind, hat der Schutz der Persönlichkeitsrechte und der Privatsphäre sowie der informationellen Selbstbestimmung der betroffenen Person bei der Beurteilung wesentlich ins Gewicht zu fal- len. Es wären damit hohe Hürden an die Verhältnismässigkeit solcher Datenbearbeitungen zu stellen.

Die Datenbearbeitung kann schliesslich auch durch Gesetz gerechtfertigt sein, wobei als Rechtfertigungsgrund für eine allfällige Persönlichkeitsverletzung nur eine *Rechtsgrundlage im schweizerischen Recht* in Frage kommt. Da im vorliegenden Kontext ein US-Rechtsakt, nämlich der *CLOUD Act*, als Rechtsgrundlage für die Anordnungen dient, könnte sich ein CSP nicht auf den Rechtfertigungsgrund der gesetzlichen Grundlage gemäss Artikel 13 Ab- satz 1 DSG respektive Artikel 31 Absatz 1 nDSG berufen. Dies würde sich voraussichtlich erst durch den Abschluss eines umfassenden Staatsvertrages mit den USA im Bereich des Datenaustauschs inkl. entsprechender Schutzstandards ändern, welcher den Anforderungen an grenzüberschreitende Datenbekanntgaben (Art. 6 Abs. 2 Bst. a DSG bzw. Art. 16 Abs. 2 Bst. a nDSG) genügt. Ein blosses *Executive Agreement* gemäss *Cloud Act* vermöchte diese Anforderungen kaum zu erfüllen.

5.5.2.4 Vereinbarkeit mit den Anforderungen an grenzüberschreitende Datenbekanntgaben (Art. 6 DSG/Art. 16 und 17 nDSG)

Weil Personendaten durch die Bekanntgabe ins Ausland nicht mehr dem Schutz der schwei- zerischen Datenschutzgesetzgebung unterstehen, sondern einer ausländischen Rechtsord- nung unterstellt werden, erhöht sich das Risiko von Persönlichkeitsverletzungen. Art. 6

¹¹⁶ ROSENTHAL, JÖHRI, Art. 13, Rz. 14 verweisen diesbezüglich auf die bundesgerichtliche Rechtsprechung in BGE 97 II 106 f.

¹¹⁷ MAURER-LAMBROU, STEINER, «Art. 6 DSG», Rz. 32.

¹¹⁸ ROSENTHAL, JÖHRI, Art. 6, Rz. 60. Ebenso BAERISWYL, B., BLONSKI, D., «Art. 6», in Baeriswyl, B. (Hrsg.), *Datenschutzgesetz – Stämpfli Handkommentar*, Bern: Stämpfli 2015, Rz. 30.

¹¹⁹ Siehe z. B. ROSENTHAL, JÖHRI, Art. 6, Rz. 61.

Bericht zum US Cloud Act

DSG stellt Anforderungen an solche Datenbekenntgaben, durch welche die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. Letztere ist von Gesetzes wegen grundsätzlich dann anzunehmen, wenn der betreffende Staat nicht über eine Gesetzgebung verfügt, die einen angemessenen Datenschutz gewährleistet, also einen dem schweizerischen Recht vergleichbaren Schutz gewährleistet. Bei den USA ist dies nicht der Fall. So wird das Datenschutzniveau der USA vom EDÖB inzwischen *in keinem Bereich mehr als angemessen* angesehen.

Da bereits festgestellt wurde, dass Datenbearbeitungen gestützt auf Herausgabeanordnungen im Hinblick auf die datenschutzrechtlichen Grundsätze generell als problematisch anzusehen sind und von deren Rechtswidrigkeit gemäss schweizerischem Datenschutzrecht auszugehen ist, erübrigen sich mit Bezug auf die Vereinbarkeit mit den Anforderungen an grenzüberschreitende Datenbekenntgaben detaillierte Ausführungen.

Zusammenfassend kann aber Folgendes festgehalten werden: Auch bei Fehlen eines angemessenen Schutzes im Ausland können Datenbekenntgaben ausnahmsweise zulässig sein, nämlich dann, wenn rechtlich bindende und durchsetzbare Instrumente geeignete Garantien für einen angemessenen Schutz der Daten im Ausland vorsehen, wenn die betroffene Person in die Bekanntgabe einwilligt, wenn die Datenbekenntgabe unerlässlich ist zur Wahrung eines überwiegenden öffentlichen Interesses oder zur Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht oder erforderlich zum Schutz des Lebens oder der körperlichen Integrität der betroffenen Person oder eines Dritten.

Konkret wäre im Einzelfall denkbar, dass CSP Personendaten an US-Strafverfolgungsbehörden bekannt geben, sofern dies zum Schutz der lebenswichtigen Interessen der betroffenen Person selbst, oder im Rahmen konkreter laufender Strafverfahren für die Durchsetzung von Rechtsansprüchen unerlässlich ist. Ausserdem könnten sich CSP auch auf ausländische Sicherheitsinteressen berufen, um ein öffentliches Interesse aus Sicht der Schweiz geltend zu machen. In jedem Fall aber müssen die betroffenen Interessen vorsichtig gegeneinander abgewogen werden. Da prinzipiell von einer schwerwiegenden Gefährdung der Persönlichkeitsrechte der betroffenen Personen auszugehen ist, deren Personendaten an US-Strafverfolgungsbehörden gestützt auf Herausgabeanordnungen bekannt gegeben werden, sollten diese Ausnahmefälle generell aber nur mit Zurückhaltung als Rechtfertigungsgründe für solche Datenbekenntgaben angenommen werden.

5.5.2.5 Weitere aus datenschutz- und grundrechtlicher Sicht problematische Aspekte

Daneben lassen sich auch weitere aus datenschutz- und grundrechtlicher Sicht problematische Aspekte im Zusammenhang mit solchen Datenbearbeitungen aufführen. Mit Blick auf den Schutz der Privatsphäre (Art. 13 BV) sind solche Datenbearbeitungen in verschiedener Hinsicht als heikel anzusehen. Artikel 8 der Europäischen Menschenrechtskonvention (nachfolgend EMRK)¹²⁰ anerkennt das Grundrecht auf Achtung des Privatlebens. Gemäss der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (nachfolgend EGMR) muss jeder Eingriff in das Privatleben gesetzlich vorgesehen sein, einen rechtmässigen Zweck verfolgen und sich auf das in einer demokratischen Gesellschaft Erforderliche beschränken.¹²¹ In Bezug auf das Recht auf Datenschutz wendet der Gerichtshof den Ansatz der «unbedingten Erforderlichkeit» an.¹²² Sowohl der EGMR (in Anwendung der EMRK)

¹²⁰ SR 0.101

¹²¹ Zum Beispiel EGMR, *Liberty und andere gegen Vereinigtes Königreich*, Urteil vom 1. Juli 2008, Beschwerde 58243/00, ECLI:CE:ECHR:2008:0701JUD005824300.

¹²² EGMR, *Szabó und Vissy gegen Ungarn*, Urteil vom 12. Januar 2016, Beschwerde 37138/14, ECLI:CE:ECHR:2016:0112JUD003713814, S. 33; EuGH, *Digital Rights Ireland und Seitlinger u. a.*

Bericht zum US Cloud Act

als auch der EuGH (in Anwendung der Europäischen Charta) haben zahlreiche Garantien zur Kontrolle der elektronischen Kommunikation durch die Regierungen geschaffen.¹²³

Auch in diesem Zusammenhang erscheinen im Wesentlichen die gleichen Aspekte des *CLOUD Act* als besonders heikel, die bereits unter Ziffer 5.5.1.1 im Zusammenhang mit der Vereinbarkeit mit der DSGVO erwähnt wurden.¹²⁴ Es handelt sich dabei um die im *CLOUD Act* vorgesehene unterschiedliche Regelung betreffend Inhalts- und Nichtinhaltsdaten und von Daten von US-Personen und anderen Personen, die fehlende Unterscheidung zwischen Verantwortlichem und Auftragsbearbeiter, die Überwachung von Kommunikationsinhalten in Echtzeit, fehlende Rechte der betroffenen Person namentlich bezüglich Auskunft und Information sowie fehlende administrative und gerichtliche Rechtsbehelfe für die betroffene Person. Der fehlende Anspruch auf gerichtliche Beurteilung ist neben seiner Problematik aufgrund der datenschutzrechtlichen Vorgaben insbesondere auch unvereinbar mit der in Artikel 29a BV statuierten Rechtsweggarantie, wonach jede Person bei Rechtsstreitigkeiten Anspruch auf Beurteilung durch eine richterliche Behörde (in der Schweiz) hat.¹²⁵

5.5.2.6 Schlussfolgerung zur Datenschutzkompatibilität eines *Executive Agreements*

Insgesamt sind Datenbekanntgaben und -bearbeitungen gestützt auf Herausgabebeanordnungen nicht nur im Hinblick auf die Vereinbarkeit mit der DSGVO, sondern auch mit derjenigen mit dem schweizerischen Datenschutzrecht sowie allgemein aus grundrechtlicher Sicht als grundsätzlich problematisch anzusehen. Eine wichtige Voraussetzung für die Anerkennung der Angemessenheit des schweizerischen Datenschutzniveaus durch die Europäische Kommission ist schliesslich die Ratifizierung des Änderungsprotokolls zur Datenschutzkonvention des Europarates¹²⁶ («*Datenschutzkonvention 108+*»). Da die Umsetzung der konventionsrechtlich vorgeschriebenen datenschutzrechtlichen Garantien für eine Ratifizierung der Datenschutzkonvention 108+ vorausgesetzt wird (Art. 4 Abs. 2 Datenschutzkonvention 108+), ist ein Abschluss eines *Executive Agreements* auch vor diesem Hintergrund als heikel einzustufen.

Mangels angemessenen Datenschutzes in den USA ist davon auszugehen, dass Datenbekanntgaben an US-Strafverfolgungsbehörden einen schwerwiegenden Eingriff in die Persönlichkeitsrechte der betroffenen Personen darstellen würden. Vorbehaltlich einer eingehenderen Prüfung kann angenommen werden, dass deren allfällige Einwilligung vermutlich keinen gültigen Rechtfertigungsgrund darstellen würde. Denkbar wäre zwar, dass ein CSP eine solche Datenbekanntgabe mit den Sicherheitsinteressen der USA rechtfertigen könnte. Ein denkbarer Rechtfertigungsgrund wäre auch, dass die Bekanntgabe im Interesse der betroffenen Person selbst (d. h. zum Schutz ihrer eigenen lebenswichtigen Interessen oder zur Durchsetzung von Rechtsansprüchen in einem konkreten Strafverfahren) erfolgen würde. Aber selbst hier müsste bei der Interessenabwägung wesentlich ins Gewicht fallen, dass die Datenbekanntgabe die Persönlichkeit der betroffenen Person schwerwiegend gefährden würde.

Namentlich im Hinblick auf die datenschutzrechtlichen Grundsätze der Transparenz und Verhältnismässigkeit sind Datenbearbeitungen gestützt auf Herausgabebeanordnungen als problematisch anzusehen. Selbst wenn auch hier im Einzelfall nicht auszuschliessen wäre, dass

¹²³ EGMR, *Roman Zakharov gegen Russland*, Urteil vom 4. Dezember 2015, Beschwerde 47143/06, E-CL:CE:ECHR:2015:1204JUD004714306.

¹²⁴ Siehe zum Folgenden namentlich das Dokument «Évaluation du CCBE de la loi CLOUD Act des États-Unis», vom 28.02.2019, Conseil des Barreaux Européens, abrufbar unter: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/FR_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf.

¹²⁵ Vgl. dazu die weiteren Ausführungen unten bei 5.6.1.

¹²⁶ SR 0.235.1

Bericht zum US Cloud Act

sich CSP auf ein schützenswertes öffentliches Interesse oder auf die Interessen der betroffenen Person selbst berufen könnten, sollte entsprechend der bundesgerichtlichen Rechtsprechung und der Haltung der europäischen Datenschutzbehörden eine Verletzung der datenschutzrechtlichen Grundsätze, die als schwerwiegender Eingriff in die Persönlichkeitsrechte der betroffenen Person anzusehen ist, nur mit grosser Zurückhaltung gerechtfertigt werden können.

Auch in Bezug auf weitere, aus datenschutz- und grundrechtlicher Sicht wichtige Kernanliegen erweisen sich Datenbearbeitungen gestützt auf Herausgabeanordnungen als bedenklich. Wesentlich ins Gewicht fallen hier insbesondere die unter dem *CLOUD Act* fehlenden Zugangs-, Berichtigungs- und Löschrechte der betroffenen Personen mit Bezug auf ihre Daten, aber auch das Fehlen von Rechtsschutzmöglichkeiten sowie von verfahrensrechtlichen Garantien. Insbesondere mit Blick auf die Rechtsweggarantie (Artikel 29a BV) erscheint ein *Executive Agreement* nach schweizerischem Recht problematisch.

5.5.3 Welcher Datenschutz müsste in einem *Executive Agreement* mit den USA aufgenommen werden?

Ein allfälliges *Executive Agreement* wäre ein völkerrechtlicher Vertrag zwischen der Schweiz und den USA. Der Vertrag sollte mithin hinreichende Garantien enthalten, damit auch für die an die US-Strafverfolgungsbehörden bekanntzugebenden Personendaten ein dem hiesigen Recht entsprechender Datenschutz- und Grundrechtsschutzstandard sichergestellt wird. Mangels entsprechender Garantien im *CLOUD Act* müssten die wesentlichsten Grundsätze und Garantien sowie die Rechte der betroffenen Personen im Abkommen selbst geregelt werden.

Es ist allerdings fraglich, ob der vom *CLOUD Act* vorgegebene Rahmen für *Executive Agreements* solche umfassenden datenschutzrechtlichen Garantien überhaupt zulässt, vor allem, weil dieses Gesetz selbst aus datenschutzrechtlicher Sicht als problematisch anzusehen ist. Erwähnenswert ist dabei insbesondere, dass eine betroffene Person selbst bei Vorliegen eines *Executive Agreements* nicht die Möglichkeit hätte, sich gegen die Bekanntgabe ihrer Personendaten zu wehren, da der *CLOUD Act* einen Abwehrmechanismus lediglich für die CSP vorsieht, und auch dies nur in einem sehr begrenzten Rahmen. Die laufenden Verhandlungen zwischen der EU und den USA (siehe Ziff. 4.2.2) zeigen denn auch die Absicht der EU, den Datenaustausch von elektronischen Beweismitteln in Strafsachen in einem umfassenden Rahmenabkommen zu regeln, welches substantiell wesentlich über ein *Executive Agreement* hinausgeht.

Der Beschluss der Europäischen Kommission vom 28. Juni 2021 über die Angemessenheit des UK Datenschutzniveaus nach der DSGVO zeigt, dass der Abschluss eines *Executive Agreements* mit den USA Folgen für die künftige Beurteilung der Angemessenheit des schweizerischen Datenschutzes haben wird. Der Entscheid des EU-Parlaments vom 21. Mai 2021, den von der Kommission vorgelegten Adäquanzentscheid des UK zurückzuweisen – u. a. mit Verweis auf «onward transfers of data to other countries and bulk access to data by law enforcement»¹²⁷ – verdeutlicht die Begründetheit dieser Annahme.

Im Unterschied zur UK, welche im Gegensatz zur Schweiz die DSGVO mit Ausnahme des Bereichs der Einwanderungskontrolle vollständig umsetzt und im UK-US *CLOUD Act Agreement* einen Verweis auf die im EU-US Rahmenabkommen gewährleisteten Rechte und Garantien durchzusetzen verspricht, muss davon ausgegangen werden, dass ein *Executive*

¹²⁷ Vgl. Pressemitteilung des EU-Parlaments vom 21.5.2021, einsehbar über: <https://www.europarl.europa.eu/news/en/press-room/20210517IPR04124/data-protection-meps-urge-the-commission-to-amend-uk-adequacy-decisions> (Stand 26.5.2021).

Agreement, welches die Schweiz im engen Rahmen des *CLOUD Acts* mit den USA abschliesse, nicht den Anforderungen der EU an ein angemessenes Datenschutzniveau genügen dürfte. In dieser Hinsicht sowie im Einklang mit den Verhandlungen zwischen der EU und den USA sollte vielmehr ein umfassendes Abkommen anvisiert werden, welches die Datenbearbeitungen und -bekanntgaben von elektronischen Beweismitteln in Strafsachen durch CSP an die US- und die schweizerischen Strafverfolgungsbehörden abschliessend regelt und ein hohes Schutzniveau für die in diesem Rahmen bearbeiteten Personendaten und die Grundrechte und -freiheiten der betroffenen Personen garantiert. Vor diesem Hintergrund liegt es im Interesse der Schweiz, die Verhandlungsergebnisse in Bezug auf das Übereinkommen zwischen der EU und den USA abzuwarten.

Zudem sollten auch die gegenwärtigen Entwicklungen auf europäischer Ebene im Zusammenhang mit dem Datenschutz weiterverfolgt werden. In seinem Urteil vom 16. Juli 2020 in der Rechtssache «Schrems II» hält der EuGH fest, dass die Bestimmungen zu den staatlichen Überwachungsprogrammen im amerikanischen Recht keine hinreichenden Garantien zur Erfüllung der Anforderungen der DSGVO an den Datenschutz und keinen genügenden Rechtsschutz für die betroffenen nichtamerikanischen Personen bieten.¹²⁸ Die Europäische Kommission stützt sich in ihren Beschlüssen über die Angemessenheit des Datenschutzniveaus von UK wesentlich auf diesen Entscheid ab. Deshalb dürfte er auch einen wesentlichen Einfluss auf die Beurteilung eines allfälligen *Agreements* mit den USA im Hinblick auf die Angemessenheit des schweizerischen Datenschutzniveaus haben. Auch die von der Europäischen Kommission durchgeführte Anpassung von EU-Rechtsakten, welche Datenbearbeitungen im Bereich der Strafverfolgung und -vollstreckung regeln, an die Richtlinie (EU) 2016/680 lässt vermuten, dass künftig Datenbekanntgaben aus der EU an Drittstaaten in diesem Zusammenhang noch strenger beurteilt werden.¹²⁹

5.6 Vereinbarkeit mit dem schweizerischen Rechtshilferecht

Die internationale Rechtshilfe in Strafsachen (akzessorische Rechtshilfe) zwischen der Schweiz und den USA wird hauptsächlich im Staatsvertrag vom 25. Mai 1973¹³⁰ zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen (nachfolgend RVUS) und im Bundesgesetz vom 3. Oktober 1975¹³¹ zu diesem Gesetz (nachfolgend BG-RVUS) geregelt. Weder im RVUS noch im BG-RVUS geregelte Aspekte werden durch das Rechtshilfegesetz (IRSG)¹³² und dessen Verordnung (IRSV)¹³³ abgedeckt. Subsidiär gilt die Strafprozessordnung (StPO)¹³⁴ für Massnahmen, die nicht direkt im IRSG geregelt sind. Für die Schweizer CSP gilt zudem das BÜPF.

Nachfolgend wird die Vereinbarkeit eines allfälligen *Executive Agreements* und des *CLOUD Acts* mit diesen rechtlichen Grundlagen geprüft. Dabei ist klar, dass sämtliche Bestrebungen im Bereich «E-Evidence» am hergebrachten rechtshilferechtlichen Rahmen rütteln. Das ist mit Blick auf die Regelungsmaterie wohl unerlässlich und durchaus so gewollt. Im vorliegenden Abschnitt wird dieser im Raum stehende «Paradigmenwechsel» weg von einer klassischen Rechtshilfe und hin zu einer direkteren Form der Zusammenarbeit dennoch aus der

¹²⁸ EuGH, *Schrems II*, E. 175-178.

¹²⁹ Mitteilung der Kommission an das Europäische Parlament und den Rat – Weiteres Vorgehen hinsichtlich der Angleichung des früheren Bestitzstands des dritten Pfeilers an die Datenschutzvorschriften, einsehbar auf https://eur-lex.europa.eu/resource.html?uri=cellar:c835f51d-b6d5-11ea-bb7a-01aa75ed71a1.0023.02/DOC_1&format=PDF (Stand 1.7.2020).

¹³⁰ SR 0.351.933.6

¹³¹ SR 351.93

¹³² SR 351.1

¹³³ SR 351.11

¹³⁴ SR 312.0

Werte der Grundsätze und Prinzipien des Schweizer Rechtshilferechts beleuchtet. Ziel ist, vor dem Hintergrund dieser Prinzipien Möglichkeiten und Schranken aufzuzeigen.

5.6.1 Gründe für die Ablehnung eines Rechtshilfeersuchens und Rechtsweggarantie

Im schweizerischen Rechtshilfeverfahren sind gewisse zwingende Ablehnungsgründe für ausländische Rechtshilfeersuchen vorgesehen. Diese sind bei Beweiserhebungsmassnahmen in der Schweiz von Amtes wegen zu prüfen und können von betroffenen Personen im hiesigen Verfahren vor schweizerischen Behörden und Gerichten geltend gemacht werden. Die Ablehnungsgründe finden sich hauptsächlich in den Artikeln 2 und 3 IRSG.¹³⁵ Für Fälle von Straftaten mit politischem, militärischem, fiskalischem¹³⁶, währungs-, handels- oder wirtschaftspolitischen Charakter wird keine Rechtshilfe geleistet, ebenso wie in Fällen, in denen das ausländische Verfahren elementare Grundsätze verletzt oder generell schwere Mängel aufweist. Dies ist etwa dann der Fall, wenn das ausländische Verfahren den Verfahrensgrundsätzen der EMRK zuwiderläuft, das Verfahren durchgeführt wird, um die verfolgte Person wegen ihrer politischen Anschauungen, ihrer Zugehörigkeit zu einer bestimmten sozialen Gruppe oder aus Gründen der Rasse, der Religion oder der Volkszugehörigkeit zu bestrafen oder dazu führen könnte, dass ihre Situation aus einem dieser Gründe erschwert wird.

Hintergrund für diese Ablehnungsgründe ist letztlich Artikel 5 BV, der eine umfassende Bindung staatlichen Handelns an das Recht – inklusive Völkerrecht – statuiert. Mit einem *Executive Agreement* würden nun die (digitalen) Informationen und Beweismittel nicht mehr in einem schweizerischen Verwaltungsverfahren von einer schweizerischen Behörde erhoben, sondern der in der Schweiz domizilierte CSP würde direkt am US-Strafverfahren mitwirken. Mit der Herausgabe von Daten Dritter (seiner Kunden) zugunsten eines ausländischen Strafverfahrens, in welchem diese als Beweismittel verwendet werden können, nähme der CSP voraussichtlich eine hoheitliche Aufgabe wahr. Das *Executive Agreement* würde diese nach schweizerischem Recht staatliche Aufgabe an einen Privaten – eben den CSP – delegieren. Daher bliebe der CSP an die Grundrechte gebunden. Folglich dürfte ein *Executive Agreement* nicht hinter den aus Grundrechtssicht gebotenen Schutz – also wohl den heutigen Schutzstand im geltenden Rechtshilferecht – zurückfallen.

Es müssten daher aus schweizerischer Sicht Wege gefunden werden, diese Ausschlussgründe auch im neuen, direkten Verfahren unter dem *CLOUD Act* effizient sicherzustellen. Es geht dabei letztlich um die Sicherung des «*ordre public*».¹³⁷ Das trifft namentlich auf die politischen und fiskalischen Straftaten zu. Entsprechende Ausschlussgründe müssten voraussichtlich auch in einem allfälligen *Executive Agreement* zwischen der Schweiz und den USA enthalten sein. Ebenfalls muss die Schweiz auf jeden Fall die EMRK-Mindestgarantien beachten. Auch diese müssten daher umfassend in einem *Executive Agreement* verankert werden.

Es stellt sich die Frage, in welchem Verfahren die Einhaltung solcher Ausschlussgründe sichergestellt werden könnte. Grundsätzlich ist unter dem *CLOUD Act* gar kein schweizerisches Verfahren und keine Involvierung schweizerischer Behörden mehr angedacht. Einzig der CSP könnte im US-Verfahren und vor einem US-Gericht geltend machen, die Verwendung der Daten verstosse gegen den in der Schweiz geltenden «*ordre public*». Eine so weitgehende Unterwerfung unter fremdes Recht und fremde Gerichte ist die Schweiz bislang noch nicht eingegangen. Es ist – insbesondere mit Blick auf die verfassungsmässig garantierte Rechtsweggarantie in Artikel 29a BV – höchst fraglich, ob ein derartiges Verfahren

¹³⁵ Sie werden in dieser Form jeweils auch in die modernen bilateralen Rechtshilfeverträge der Schweiz aufgenommen. Im älteren RVUS werden diese unter die generell gehaltene Ausschlussklausel der «ähnlichen wesentlichen Interessen» gemäss Art. 3 Abs. 1 Bst. a subsumiert.

¹³⁶ Mit Ausnahme von Abgabebetrug, wo Rechtshilfe geleistet werden kann, vgl. Art. 3 Abs. 3 IRSG.

¹³⁷ ZIMMERMANN, Rz. 612.

in einem allfälligen *Executive Agreement* verfassungskonform umsetzbar wäre. Vielmehr ist davon auszugehen, dass – wie es bereits beim Datenschutz angeklungen ist – ein weiterer Rahmen erforderlich wäre, als ihn ein *Executive Agreement* unter dem *CLOUD Act* vorsieht.

5.6.2 Grundsatz der beidseitigen Strafbarkeit

Nach dem Grundsatz der beidseitigen Strafbarkeit kann eine Zwangsmassnahme auf Ersuchen eines anderen Staates nur dann vollstreckt werden, wenn die betreffende Tat sowohl im ersuchenden Staat als auch im ersuchten Staat strafbar ist. Die Zusammenarbeit nach dem *CLOUD Act* beinhaltet allerdings keine Zwangsmassnahmen. Der Begriff des *serious crime* soll die Zusammenarbeit nach dem *CLOUD Act* auf die «wichtigsten» Straftaten beschränken. Im *Executive Agreement* zwischen dem UK und den USA wird der Begriff *serious crime* anhand der drohenden Freiheitsstrafe definiert. Das *Agreement* zwischen UK und den USA geht dabei jedoch nicht vom Erfordernis der beidseitigen Strafbarkeit aus. Dieser Punkt ist verschiedentlich kritisiert worden.¹³⁸ Im Ergebnis bedeutet das, dass eine Straftat, die in den USA mit mindestens drei Jahren Freiheitsstrafe bestraft wird, Anlass zu einer Herausgabeanordnung an einen CSP in UK geben kann und dieser der Anordnung nachkommen muss, unabhängig davon, ob die Straftat in UK strafbar ist oder nicht. Namentlich mit Blick auf Steuerdelikte könnte dieser Punkt für die Schweiz mit Blick auf ein allfälliges *Executive Agreement* besonders problematisch sein.

Mit Blick auf das im Rechtshilferecht bekannte Erfordernis der beidseitigen Strafbarkeit stellt sich für die Schweiz im Zusammenhang mit dem *CLOUD Act* somit die Frage, ob eine entsprechende Zusammenarbeit trotz fehlender Strafbarkeit in der Schweiz denkbar wäre. Wird diese Frage verneint, müsste der im *Executive Agreement* zu definierende Begriff des *serious crime* um eine Dimension der beidseitigen Strafbarkeit erweitert werden. Erneut stellt sich allerdings die Frage, wie diese ohne schweizerisches Verfahren überprüft und bei Bedarf durchgesetzt werden könnte. Ob es genügt, wenn der CSP – nicht einmal der Betroffene selbst – im US-Strafverfahren geltend machen kann, das entsprechende Steuerdelikt sei in der Schweiz nicht rechtshilfefähig, ist eine Frage der politischen Bewertung.

5.6.3 Anspruch auf rechtliches Gehör

Mit Blick auf das rechtliche Gehör wird erneut die Bundesverfassung relevant. Der in Artikel 29 Absatz 2 BV verankerte Anspruch auf rechtliches Gehör garantiert, dass die einzelne Person sich äussern kann, bevor ein Entscheid zu ihrem Nachteil gefällt wird, dass sie Zugang zu den Akten erhält, Beweismittel zum Sachverhalt, die einen Einfluss auf den Entscheid haben könnten, einreichen oder beantragen kann sowie an der Beweiserhebung mitwirken, die Beweise zur Kenntnis nehmen und dazu Stellung nehmen kann.

Im Bereich der zwischenstaatlichen Zusammenarbeit in Strafsachen sind diese Anforderungen in Artikel 29 ff. VwVG und einigen Sonderbestimmungen des IRSG und des BG-RVUS konkretisiert.

Im heutigen Rechtshilfeverfahren mit den USA umfasst der Anspruch auf rechtliches Gehör zusammengefasst den Anspruch auf einen Rechtsbeistand (Art. 21 IRSG), auf Akteneinsicht (Art. 26 und 27 VwVG durch Verweis von Art. 9 BG-RVUS) und Mitwirkung bei der Ausführung des Ersuchens (Art. 12 Abs. 2 und Art. 18 Abs. 1 RVUS), den Anspruch jeder persönlich und direkt von einer Rechtshilfemassnahme betroffenen Person, die ein schutzwürdiges Interesse an deren Aufhebung oder Änderung hat, auf eine begründete Verfügung im Hinblick auf

¹³⁸ Z. B. von Human Rights Watch, abrufbar im Internet unter: <https://www.hrw.org/news/2019/10/29/groups-urge-congress-oppose-us-uk-cloud-act-agreement>.

Bericht zum US Cloud Act

die Geltendmachung ihres Beschwerderechts (Art. 17 f. BG-RVUS) sowie den Anspruch auf eine Rechtsmittelbelehrung (Art. 22 IRSG).

Grundsätzlich würde es der *CLOUD Act* der zuständigen Behörde in der Schweiz (die im *Executive Agreement* bestimmt würde) ermöglichen, die CSP mit Sitz in den USA direkt um Informationen und Daten zu ersuchen, die auf ihren Servern gespeichert sind, und die amerikanischen Behörden könnten die CSP mit Sitz in der Schweiz direkt um auf ihren Servern gespeicherte Daten ersuchen. Dieses System hätte zur Folge, dass weder die (natürlichen und juristischen) Personen, um deren Daten ersucht wird, noch eine andere Behörde (z. B. das BJ als Aufsichtsbehörde oder Zentralstelle) über eine Bekanntgabe von Daten oder Informationen informiert würden. Sie könnten nicht aktiv verlangen, über die Bekanntgabe ihrer Daten informiert zu werden¹³⁹ und könnten zu einer entsprechenden Datenbekanntgabe auch nicht Stellung nehmen. Folglich könnte der Anspruch einer direkt von der Bekanntgabe betroffenen Person oder Behörde auf rechtliches Gehör nicht gewährleistet werden.

Da der *CLOUD Act* grundsätzlich nicht vorsieht, dass die betroffene Person/Behörde Anspruch auf rechtliches Gehör hat, stellt sich die Frage, ob dieser Anspruch der betroffenen Personen/Stellen in einem *Executive Agreement* vorgesehen werden könnte. Selbst wenn dies bejaht würde, würde sich erneut die Frage stellen, wie dieser Anspruch ohne schweizerisches Verfahren sichergestellt werden könnte. Auch mit Blick auf Artikel 29 Absatz 2 BV wäre ein *Executive Agreement* kaum verfassungsmässig umsetzbar. Der vertragliche Rahmen müsste ausgedehnt werden.

5.6.4 Aufsichts- und Kontrollbehörde

In erster Linie ist das BJ zuständig für die Ausführung der Abkommen und der Gesetze im Bereich der zwischenstaatlichen Zusammenarbeit in Strafsachen (Art. 17 Abs. 2 IRSG und Art. 7 Abs. 6a der Organisationsverordnung vom 17. November 1999¹⁴⁰ für das Eidgenössische Justiz- und Polizeidepartement, nachfolgend OV-EJPD). Im Rahmen der internationalen Rechtshilfe in Strafsachen mit den USA erfüllt es die Funktion der Zentralstelle nach Artikel 28 Absatz 1 RVUS sowie die Funktion der Aufsichtsbehörde, die ihm aufgrund seiner Legitimation zur Beschwerde gegen Verfügungen der ausführenden Behörde des Kantons oder des Bundes zukommt (Art. 19 Abs. 1 erster Satz BG-RVUS). Es ist ausserdem berechtigt, beim Bundesgericht gegen Verfügungen des Bundesstrafgerichts Beschwerde zu erheben (Art. 19 Abs. 1 erster Satz BG-RVUS).

Zusätzlich zur Möglichkeit, Beschwerde zu erheben, nimmt das BJ seine Aufsichtspflicht während des gesamten Rechtshilfeverfahrens in der Schweiz wahr. Dies namentlich dann, wenn es bei Erhalt eines Rechtshilfeersuchens prüft, ob die Voraussetzungen für ein Eintreten auf das Ersuchen erfüllt sind, wenn es die Verfügungen der ausführenden Behörden (namentlich kantonale Staatsanwaltschaften und Bundesanwaltschaft) auf die korrekte Anwendung des Rechtshilferechts prüft und wenn es die Informationen und Beweismittel mit dem Hinweis übermittelt, wie sie die ersuchende Behörde gemäss dem Grundsatz der Spezialität verwenden darf (Art. 5 RVUS). Das BJ überwacht ausserdem die ausgehenden Rechtshilfeersuchen (Art. 30 IRSG).

Grundsätzlich könnten die zuständigen Schweizer Behörden gemäss dem *CLOUD Act* die US-CSP direkt um Daten ersuchen und umgekehrt. So werden die Schweizer CSP Heraus-

¹³⁹ Gemäss Art. 3 Abs. 1 Bst. a Ziff. 3 Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (BGÖ, SR 152.3) sind die Verfahren der internationalen Rechts- und Amtshilfe auch vom Anwendungsbereich dieses Gesetzes ausgenommen. Die Zugangsrechte zu den Daten richteten sich daher voraussichtlich bloss nach den in einem *Executive Agreement* vorgesehenen Regeln.

¹⁴⁰ SR 172.213.1

Bericht zum US Cloud Act

gabeanordnungen der USA erhalten, von denen das BJ voraussichtlich keine Kenntnis erlangt und bei denen es folglich seine Aufsichtspflicht nicht wahrnehmen kann. Demgegenüber wird die Behörde, die im *Executive Agreement* dafür zuständig erklärt wird, in der Schweiz Herausgabeanordnungen anzuordnen, gleichzeitig ausführende Behörde sein und allein die Achtung des Rechts garantieren müssen.

Der *CLOUD Act* versieht die CSP hinsichtlich der eingehenden Ersuchen folglich mit einer Schlüsselrolle. Denn sie allein würden Kenntnis vom Ersuchen der USA erhalten und hätten die Kontrolle über das darauf folgende Verfahren.¹⁴¹ Den kleineren Dienst Anbietern könnte es an Fachwissen und Ressourcen für diese Rolle mangeln.¹⁴² Bei ausgehenden Ersuchen fiel diese Rolle den ausführenden Behörden zu.

Obwohl eine Herausgabeanordnung grundsätzlich einer gewissen Kontrolle unterliegen dürfte,¹⁴³ sieht der *CLOUD Act* scheinbar nicht vor, dass eine eigentliche Aufsichtsbehörde eingerichtet wird. Da einer der Zwecke des *CLOUD Act* darin zu bestehen scheint, dass Informationen und Daten unmittelbar und rasch ausgetauscht werden können, würde ein Aufsichtssystem den Austausch auch verlangsamen. Doch wie im Abkommen zwischen dem UK und den USA scheint es nicht ausgeschlossen zu sein, einen eingeschränkten Kontrollmechanismus einzuführen (vgl. oben, 4.1.), wenn er im *Executive Agreement* vorgesehen ist.

Es stellt sich somit die Frage, ob – entgegen dem eigentlichen Konzept gemäss *CLOUD Act* – in einem *Executive Agreement* eine Aufsichts- oder Kontrollbehörde für ein- und ausgehende Ersuchen eingerichtet werden könnte. Eine solche wäre voraussichtlich unabdingbar, um die Verfassungsmässigkeit der Zusammenarbeit zu gewährleisten (vgl. dazu unten, 5.6.8.). Zu definieren wäre, welche Stelle diese Aufsicht wahrnehme sowie welche Rolle und welche konkreten Kontrollmöglichkeiten sie hätte.

5.6.5 Grundsatz der Spezialität

Im Bereich der Rechtshilfe hat der Grundsatz der Spezialität zur Folge, dass der ersuchende Staat Schriftstücke, Informationen und Auskünfte nicht zur Verfolgung von Straftaten verwenden darf, für welche die Schweiz die Zusammenarbeit ausgeschlossen hat. Das betrifft politische, militärische, fiskalische,¹⁴⁴ währungs-, handels- und wirtschaftspolitische Delikte oder Fälle, in denen die Gewährung der Zusammenarbeit die Souveränität, die Sicherheit, die öffentliche Ordnung oder andere wesentliche Interessen des ersuchten Staates beeinträchtigen würde.¹⁴⁵ Der Grundsatz der Spezialität schützt sowohl die schweizerische Souveränität als auch die von den Rechtshilfehandlungen betroffene Person. Er gilt für den ersuchenden Staat sowie für jeden Drittstaat, der über ihn Kenntnis von den Auskünften und Informationen erlangen könnte.

Der Grundsatz der Spezialität gilt grundsätzlich auch im Verkehr mit den USA.¹⁴⁶ Obwohl die Regierungsbehörden, die mittels *Executive Agreement* ermächtigt würden, im Sinne des Abkommens um Daten zu ersuchen, über einen rechtlich eindeutig definierten Auftrag und na-

¹⁴¹ Siehe in diesem Sinn BISMUTH, S. 685.

¹⁴² BISMUTH, S. 685.

¹⁴³ *CLOUD Act*, § 2523 (b) (3) (D) (v).

¹⁴⁴ Rechtshilfe ist bei Abgabebetrug möglich, vgl. Art. 3 Abs. 3 IRSG.

¹⁴⁵ Vgl. Art. 2 des Europäischen Übereinkommens vom 20. April 1959 über die Rechtshilfe in Strafsachen (EUeR, SR 0.351.1) sowie Art. 1a und 3 IRSG.

¹⁴⁶ Vgl. Art. 5 Abs. 1 RVUS sowie Art. 67 IRSG. Zu den Einschränkungen, vgl. ZIMMERMANN, Rz. 734 mit weiteren Hinweisen.

mentlich in Bezug auf die Verwendung der Daten über klare Verfahren verfügen müssen,¹⁴⁷ scheint der *CLOUD Act* keine Bestimmung des Typs «Grundsatz der Spezialität» zu enthalten, zumindest nicht eine klare und wirksame Regelung zur erlaubten bzw. untersagten Verwendung der erhaltenen Daten.

In das Abkommen zwischen dem UK und den USA wurde eine Möglichkeit aufgenommen, die bereits im *CLOUD Act* vorgesehen ist: Die gestützt auf das Abkommen erhaltenen Daten dürfen nicht ohne Zustimmung des Staates, in dem der CSP seinen Sitz hat, an einen Drittstaat weitergegeben werden (Art. 8 Abs. 2). Gemäss dem Abkommen muss der Drittstaat zudem informiert werden, wenn die Person, um deren Informationen ersucht wird, sich nicht im UK befindet oder keine *US person* ist.¹⁴⁸ Wenn die Daten Straftaten betreffen, die in den USA zur Todesstrafe oder im UK zur Verletzung der Meinungsäusserungsfreiheit nach US-Verständnis führen könnten, muss die Zentralbehörde des anderen Staates benachrichtigt werden und zustimmen (Art. 8 Abs. 4). Die gestützt auf den *CLOUD Act* erhaltenen Daten dürfen, wie in Ziffer 4.1 erwähnt, nicht ohne vorgängige Einwilligung des anderen Staates zur Verhängung der Todesstrafe in den USA oder zur Verletzung der Meinungsäusserungsfreiheit im UK verwendet werden. Das UK hat folglich ein Vetorecht hinsichtlich der Verwendung von Beweismitteln in Verfahren, in denen die Todesstrafe beantragt wurde.

Grundsätzlich verlöre die Schweiz mit einem *Executive Agreement* weitgehend die Kontrolle über die Verwendung der bekannt gegebenen Daten. Dies umso mehr, wenn darin nicht eine schlagkräftige Aufsichtsbehörde (im weiteren Sinn) eingesetzt würde. Es erscheint überdies fraglich, ob der Grundsatz der Spezialität im bisherigen Sinne (also inkl. beispielsweise des Ausschlusses für fiskalische Delikte) in einem *Executive Agreement* verankert werden könnte. Vor allem aber stellt sich die Frage, wie dessen Anwendung – ausschliesslich noch in einem US-Verfahren und nur durch den betroffenen CSP als Partei – in einem mit dem geltenden höherrangigen Schweizer Recht vereinbaren Umfang durchgesetzt werden könnte.

5.6.6 Begrenzung der Zusammenarbeit aus «politischen» Gründen

Es ist bereits angeklungen, dass die Schweiz die Rechtshilfe auch dann verweigern kann, wenn diese die Hoheitsrechte, die Sicherheit, die öffentliche Ordnung oder andere wesentliche Interessen der Schweiz zu verletzen droht.¹⁴⁹ Dies geschieht i. d. R. auf entsprechende Rüge der betroffenen Partei. Die Rechtshilfe kann auch an Bedingungen geknüpft werden, wenn solche Interessen betroffen sind.¹⁵⁰ Die Entscheidkompetenz liegt in diesen Fällen beim EJPD, welches die anderen Departemente in seinen Entscheid einbezieht. Der Entscheid des EJPD unterliegt der Beschwerde an den Bundesrat. Eine solche «Souveränitätsschutz-Klausel» wäre kaum mit dem *CLOUD Act* vereinbar.

5.6.7 Vereinbarkeit mit der Strafprozessordnung und dem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs

Bei der Ausarbeitung eines bilateralen Abkommens wäre auch darauf zu achten, dass die darin enthaltenen Bestimmungen vereinbar sind mit den einschlägigen Normen der StPO¹⁵¹, den übrigen anwendbaren Erlassen im Bereich des Strafprozesses sowie des

¹⁴⁷ *CLOUD Act*, § 2523 (b) (1) (B) (iv)

¹⁴⁸ Art. 5 des Abkommens. Siehe ebenfalls DASKAL, SWIRE, «The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards»; Drittstaat ist in diesem Kontext der Staat, dessen Staatsangehörigkeit die betroffene Person hat.

¹⁴⁹ Art. 1a IRSG; vgl. auch Art. 3 Abs. 1 Bst. a RVUS.

¹⁵⁰ ZIMMERMANN, Rz. 714.

¹⁵¹ Die wichtigsten Voraussetzungen der StPO für die Überwachung des Fernmeldeverkehrs lauten wie folgt: Anordnung der Überwachung durch die Staatsanwaltschaft (Art. 269 Abs. 1 Einleitungssatz, Art. 273 Abs. 1 StPO); dringender Verdacht der Begehung einer Straftat gemäss dem Katalog nach Art. 269 Abs. 2 StPO für die Überwachung des Inhalts des Fernmeldeverkehrs (Art. 269 Abs. 1 Bst. a StPO) oder eines Verbrechens, Vergehens oder einer Übertretung nach Art. 179^{septies} StGB für die Überwachung der Randdaten (Art. 273

Bericht zum US Cloud Act

BÜPF¹⁵². Auf jeden Fall müsste darauf geachtet werden, dass die ausländischen Strafverfolgungsbehörden nicht umfassendere Kompetenzen und Möglichkeiten erhalten als die nationalen Behörden. Das bedeutet zum Beispiel, dass die US-Strafverfolgungsbehörden nicht weiter gefasste (grenzüberschreitende) Herausgabeanordnungen erlassen dürfen als die schweizerischen Strafverfolgungsbehörden gegenüber den CSP in der Schweiz oder dass der Rechtsschutz bei amerikanischen Herausgabeanordnungen nicht stärker eingeschränkt sein darf als bei nationalen Massnahmen.¹⁵³

Diese Vorgabe führt mit Blick auf das System des *CLOUD Act* zu Schwierigkeiten. Die Anforderungen der StPO und des BÜPF müssten in den amerikanischen Strafverfahren angewendet werden, auch was die Zufallsfunde (Art. 243 und Art. 278 StPO), das Verbot der Verwertung von Beweismitteln usw. betrifft, da es ja keine schweizerischen Verfahren mehr gäbe.

Vor diesem Hintergrund wäre das Verfahren nach *CLOUD Act* auch in einem allfälligen *Executive Agreement* kaum in einer Art und Weise regelbar, wie es den genannten gesetzlichen Grundlagen in der Schweiz entspricht. Wenn eine schweizerische Behörde eine Aufsichtsfunktion als Zentralbehörde für die Beschaffung von Daten durch die USA wahrnähme, könnte zwar eine vorgängige Überprüfung wahrgenommen und beim Versand der Daten etwa auf den Grundsatz der Spezialität hingewiesen werden. Selbst auf diesem Weg wäre die Einhaltung der Anforderungen an die nationalen Verfahren jedoch nicht gewährleistet. U.a. ist kaum denkbar, dass auf diesem Weg ein umfassendes Beschwerderecht eingerichtet werden könnte.

Es ist in diesem Zusammenhang zu prüfen, ob die wesentlichen geltenden Bestimmungen im Bereich der grenzüberschreitenden Übergabe von «E-Evidence» nicht eher in einem nationalen Gesetz geregelt werden sollten. Dieses Regime könnte dann als Grundlage für eine unbestimmte Anzahl künftiger bilateraler Abkommen dienen. Entsprechend sind z. B. UK und Australien vorgegangen. Selbst auf diesem Weg, wo zunächst auf gesetzgeberischem Weg grundlegende «Systemkompatibilität» hergestellt würde, wären anschliessend im Rahmen eines *Executive Agreements* noch weitere rechtliche Fragen zu klären. Zunächst müsste die konkrete Interaktion der Rechtssysteme definiert werden, und daneben wäre eine Reihe von technischen Aspekten zu regeln, z. B. die Frage, wie es sich mit der Aufbewahrungsfrist für die Randdaten verhält bzw. ob diese auch für die US-CSP gilt. Das Schweizer Recht sieht eine Aufbewahrungsfrist sowie eine Dauer für die rückwirkende Überwachung vor. Das scheint in den USA nicht grundsätzlich der Fall zu sein. Was also gälte im bilateralen Verhältnis?

Abs. 1 StPO); die Schwere der Straftat rechtfertigt die Überwachung (Achtung des Grundsatzes der Verhältnismässigkeit: Art. 269 Abs. 1 Bst. b. StPO); Achtung des Grundsatzes der Subsidiarität (Art. 269 Abs. 1 Bst. c StPO); Genehmigung durch das Zwangsmassnahmengericht (Art. 272 Abs. 1 und 273 Abs. 2 StPO); Umgang mit nicht benötigten Ergebnissen (Art. 276 StPO); Verwertbarkeit von Ergebnissen aus nicht genehmigten Überwachungen (Art. 277 StPO); Regelung der Zufallsfunde (Art. 278 StPO); Mitteilung der Überwachung (Art. 279 Abs. 1 und 2 StPO); Beschwerde (Art. 279 Abs. 3 StPO).

¹⁵² Die wichtigsten Voraussetzungen des BÜPF für die Überwachung des Fernmeldeverkehrs lauten wie folgt: Der Dienst ÜPF ist sozusagen die Schnittstelle zwischen den Strafverfolgungsbehörden und den Anbietern (Überwachungsanordnung wird nicht direkt von der Strafverfolgungsbehörde an den Anbieter übermittelt, sondern an den Dienst ÜPF, der in der Folge eine entsprechende Verfügung [Art. 5 VwVG] an den betreffenden Dienstanbieter übermittelt; die vom Anbieter gelieferten Daten werden nicht direkt an die zuständige Strafverfolgungsbehörde übermittelt, sondern an den Dienst ÜPF, der sie danach der zuständigen Strafverfolgungsbehörde zur Verfügung stellt); spezifische Pflichten der verschiedenen Kategorien von Anbietern, die im Gesetz und den entsprechenden Verordnungen genannt werden, mehr oder weniger umfangreiche Pflichten je nach Art des Anbieters; Entschädigung des Anbieters für jede Überwachung, wird vom Dienst ÜPF entrichtet und durch einen Teil der Gebühr finanziert, die von der Strafverfolgungsbehörde an den Dienst ÜPF bezahlt wird; Beschwerde des Anbieters gegen die Verwaltungsverfügung des Dienstes ÜPF (es können keine Rügen im Zusammenhang mit dem Strafverfahren geltend gemacht werden).

¹⁵³ Vgl. z.B. Art. 274 sowie 279 StPO.

5.6.8 Welche «rechtshilferechtlichen» Inhalte müssten in ein *Executive Agreement* aufgenommen werden?

Auch beim und nach dem Abschluss eines *Executive Agreements* bliebe die Schweiz an ihre grund- und menschenrechtlichen Verpflichtungen gebunden. Es müssten daher aus rechtlicher Sicht zwingend Wege gefunden werden, wie die verfassungsmässigen Garantien des *rechtlichen Gehörs* (Art. 29 Abs. 2 BV) und der *Rechtsweggarantie* (Art. 29a BV) gewahrt blieben. Auch die verfahrensmässigen *Mindestgarantien gemäss EMRK* sowie der schweizerische «*ordre public*» (u. a. mit Blick auf den Ausschluss der Rechtshilfe im Bereich von politischen oder fiskalischen Delikten) müssten garantiert werden können. Ebenfalls wäre sicherzustellen, dass ein allfälliges *Executive Agreement* die US-Strafverfolgungsbehörden gegenüber den schweizerischen Strafverfolgungsbehörden nicht ungebührlich privilegiert, was die Erhebung von Daten in der Schweiz anbelangt (vgl. dazu 5.4.3.). Es ist kaum vorstellbar, wie die diesbezüglichen Vorgaben des *schweizerischen Strafprozessrechts* allesamt in einem *Executive Agreement* verankert werden sollten. Es scheint daher unabdingbar, dass die Schweiz zunächst ihre eigenen Standards im Bereich der grenzüberschreitenden Herausgabe von «E-Evidence-System» definiert, bevor sie mittels Staatsverträgen Brücken zu den Systemen von Partnerstaaten baut. Dies würde es ausserdem ermöglichen, ein solches System eigenständig und unter Berücksichtigung des Schweizer Rechts zu gestalten, wobei die schweizerische Souveränität auch mit Blick auf eine direktere Zusammenarbeit im Bereich von «E-Evidence» in hinreichendem Masse gewahrt und wichtige schweizerische Werte geschützt blieben.

6 Datensicherheit und Entschlüsselung

6.1 Gesicherte Übermittlung

Eine Übertragung von Daten von einem Schweizer CSP an eine US-Strafverfolgungsbehörde müsste in einer mit dem Schweizer Recht konformen Art geschehen. Es wäre im Einzelfall zu prüfen, wie die Personendaten von einem CSP an eine Behörde ins Ausland übertragen werden. Bei E-Mail-basierten Systemen (oder anderen Systemen mit Zwischenservern) erscheint eine Transport- und Inhaltsverschlüsselung notwendig, um den Datenschutz während der gesamten Übermittlung zu gewährleisten. Bei einer Upload-Plattform (oder einem ähnlichen System ohne Weiterleitung der Daten an andere Systeme) erscheint die Transportverschlüsselung als ausreichend, falls die Plattform von der Behörde selbst betrieben wird. Ist der Betrieb der Upload-Plattform an Dritte ausgelagert, erscheint auch eine Inhaltsverschlüsselung erneut als notwendig.

Werden besonders schützenswerte Personendaten übertragen – was im Rahmen von Strafverfahren der Regelfall sein dürfte – so sieht der Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes des EDÖB vor, dass die Personendaten stets inhaltsverschlüsselt sein müssen¹⁵⁴.

Es müssten in einem *Executive Agreement* demnach auch Regelungen gefunden werden, die diese schweizerischen Standards für die Übermittlung der Daten an eine US-Strafverfolgungsbehörde respektieren. Die Ergebnisse der Verhandlungen zwischen der EU und den USA im Bereich Datenschutz dürften für die Schweiz diesbezüglich nützlich sein.

¹⁵⁴ EDÖB, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, August 2015, S. 20, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/datenschutz/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html>.

6.2 Neutral encryption

Von der Frage der rechtskonformen, sicheren Übermittlung der Daten von einem Schweizer CSP an die US-Strafverfolgungsbehörden oder umgekehrt zu unterscheiden ist die Frage der verschlüsselten Aufbewahrung der Daten *beim CSP*.

Die CSP können eine Vielzahl von Dienstleistungen anbieten, die dem Bedürfnis nach Datensicherheit von (Kunden-)Daten gerecht werden. Dazu gehören Verschlüsselungen. Der *CLOUD Act* sieht keine Pflicht zur Offenlegung von Verschlüsselungen vor. Er enthält insbesondere keine Bestimmung für die Entschlüsselung von Daten, welche die CSP im Namen ihrer Benutzer oder Kunden besitzen.¹⁵⁵ Die CSP können somit nicht zur Entschlüsselung von Daten gezwungen werden, die vom Kunden verschlüsselt wurden.¹⁵⁶

Zwar verpflichten beispielsweise die FINMA oder das BAG in spezialrechtlichen Bestimmungen (z. B. Art. 12 Abs. 5 der Verordnung vom 22. März 2017 über das elektronische Patientendossier [EPDV])¹⁵⁷ zur Speicherung von Kundendaten im Inland und nach schweizerischem Recht. Selbst wenn Betroffene – in diesem Falle also Finanz- bzw. Gesundheitsdienstleister – dieser Verpflichtung nachkommen und besonders schützenswerte Personendaten bei schweizerischen Datencentern hinterlegen, besteht in gewissen Situationen im Anwendungsbereich des *CLOUD Act* das Risiko eines möglichen Zugriffs auf Daten durch die US-Behörden. Bei der Auslagerung von Daten können gesetzliche und/oder vertragliche Geheimnispflichten es erfordern, dass Daten verschlüsselt gespeichert werden. Bei der Verschlüsselung bestehen verschiedene technische Vorgehensweisen, welche sich u. a. dadurch unterscheiden, ob nach *CLOUD Act* eine technische Zugriffsmöglichkeit auf die Daten besteht oder nicht.

Zu unterscheiden ist zunächst zwischen kundenseitiger Verschlüsselung und serverseitiger Verschlüsselung. Werden die Daten bereits auf dem Rechner des Kunden bzw. Datenherrs verschlüsselt und anschliessend verschlüsselt an den CSP übermittelt (kundenseitige Verschlüsselung), verbleibt der kryptographische Schlüssel beim Kunden. Dem CSP ist es nicht möglich, die Daten zu entschlüsseln. Folglich sind diese – ohne Mitwirkung des Kunden bzw. Datenherrs – weitgehend gegen einen Zugriff der US-Behörden unter dem *CLOUD Act* geschützt. Anders ist die Lage bei der serverseitigen Verschlüsselung. Bei dieser muss zwischen drei verschiedenen Varianten unterschieden werden. Zuerst gibt es die Möglichkeit, den Schlüssel durch den CSP verwalten zu lassen, d. h. der Schlüssel ist ebenfalls in der Cloud hinterlegt und der CSP hat legalen Zugriff darauf. Bei dieser Variante kann der CSP den US-Behörden den Zugriff auf verschlüsselte Daten grundsätzlich ermöglichen. Der Schutz der Kundendaten hängt vom Kooperationswillen des CSP ab, denn wie einleitend festgehalten wurde, besteht gemäss *CLOUD Act* keine Verpflichtung des CSP zur Entschlüsselung von Kundendaten. In einer zweiten Variante verwaltet der Kunde den Schlüssel zwar selbst («*Bring Your Own Key*, BYOK», manchmal auch «*Bring Your Own Encryption*, BYOE»). Dieser muss aber allenfalls in der Cloud hinterlegt und gespeichert sein. Mit der Hinterlegung des Schlüssels auf der Cloud greift der *CLOUD Act*, d. h. die Daten können vom CSP entschlüsselt und somit herausgegeben werden. Ob der CSP das darf, hängt zunächst von seinen Nutzungsbedingungen und in zweiter Linie wohl vom erzeugten Druck seitens der US-Behörden ab. In einer dritten Variante der serverseitigen Verschlüsselung wird der

¹⁵⁵ «The terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data», *CLOUD Act*, § 2523(b)(3). Siehe ebenfalls DOJ, «Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the *CLOUD Act*», S. 6; ZAGARIS, «U.S. and UK Sign Cross-Border Data Access Agreement for Cross-Border Enforcement and Warn Facebook on Proposed Encryption», S. 360.

¹⁵⁶ Gemäss Schweizer Recht können CSP nur gezwungen werden, Daten zu entschlüsseln, die sie selbst verschlüsselt haben (Art. 26 Abs. 2 Bst. c BÜPF).

¹⁵⁷ SR 816.11

kryptographische Schlüssel durch den Kunden einzig auf seiner eigenen Hardware gesichert. Bei dieser Variante besteht der gleiche Schutz wie bei der kundenseitigen Verschlüsselung. Der CSP kann die Daten nicht ohne Mitwirken des Kunden bzw. Datenherrn entschlüsseln.

Vor dem Hintergrund dieser Darstellung wird Folgendes deutlich: Zwar besteht für die CSP gemäss *CLOUD Act* keine Verpflichtung zur Entschlüsselung von Daten, welche sie im Namen ihrer Benutzer oder Kunden besitzen¹⁵⁸. Ungeachtet dieser (Nicht-)Regelung muss man sich aber bewusst sein, dass je nach technischer Möglichkeit und oder vertraglicher Abrede ein Zugriff seitens der US-Behörden auf solche Daten nicht ausgeschlossen werden kann.

7 Schlussfolgerung

Eine der derzeit grössten Herausforderungen im Bereich der zwischenstaatlichen Zusammenarbeit in Strafsachen betrifft die Sicherung und Herausgabe elektronischer Beweismittel. Es steht fest, dass in diesem Bereich neue und innovative Ansätze erforderlich sind, da ansonsten die grenzüberschreitende Strafverfolgung stark erschwert wird. Der vorliegende Bericht beleuchtet verschiedene internationale Initiativen zum erleichterten Zugang zu elektronischen Beweismitteln: Der Europarat verabschiedet ein Zweites Zusatzprotokoll zur Budapest-Konvention, die EU eine «*E-Evidence-Gesetzgebung*», in der Europäische Sicherungs- und Herausgabeanordnungen vorgesehen sind, und die UNO hat die Vorarbeiten zu einem multilateralen Übereinkommen zur Cyberkriminalität aufgenommen. Gleichzeitig sind auch auf Ebene einzelner Staaten Entwicklungen zu beobachten. Die wichtigste nationale Initiative stellt die Verabschiedung des *CLOUD Act* durch die USA dar. Dieses US-Bundesgesetz hat für die US-Strafverfolgungsbehörden und CSP extraterritoriale Wirkungen. Es erlaubt es den US-Strafverfolgungsbehörden, Zugang zu den Daten zu erhalten, die von CSP mit Sitz in den USA aufbewahrt werden – unabhängig davon, wo auf der Welt die Daten gespeichert sind. Das Gesetz bezweckt ausserdem eine «Internationalisierung» des amerikanischen Systems, da die US-Behörden die Möglichkeit erhalten, *Executive Agreements* abzuschliessen, mit denen System und Geltungsbereich des *CLOUD Act* auf andere Staaten ausgedehnt werden sollen. Da die bedeutsamsten CSP ihren Sitz in den USA haben, ist die Zusammenarbeit mit diesem Staat bezüglich der elektronischen Beweismittel namentlich für die Schweiz von besonderer Bedeutung. Aus diesem Grund stellt sich die Frage eines allfälligen Abschlusses eines *Executive Agreement* mit den USA. Der vorliegende Bericht bettet diese Frage in den grösseren Zusammenhang des «Paradigmenwechsels im Bereich der Strafrechtshilfe» ein und geht den dabei auftauchenden rechtlichen Fragen nach. Er prüft die Vereinbarkeit des *CLOUD Act* mit dem Schweizer Recht insbesondere auf zwei Ebenen: Hinsichtlich des Datenschutzes sowie der Prinzipien des Rechts der zwischenstaatlichen Zusammenarbeit in Strafsachen. Dabei gelangt das BJ zu folgenden Schlüssen:

- **Datenschutzrecht:** Die vom *CLOUD Act* erfassten Daten sind Personendaten im Sinne des Datenschutzrechts. Vor diesem Hintergrund ist es von besonderer Bedeutung, dass ein allfälliges *Executive Agreement* mit dem für die Schweiz relevanten Datenschutzrecht vereinbar ist. Das Datenschutzrecht der EU ist in der Schweiz zwar nicht direkt anwendbar, es wird im vorliegenden Bericht jedoch eingehend beleuchtet, da die Schweiz auch weiterhin von der EU als *Drittstaat mit angemessenem Datenschutzniveau (Angemessenheitsbeschluss)* anerkannt werden muss, damit sie mit den EU-Mitgliedstaaten Personendaten austauschen und am freien Datenverkehr mit der EU teilhaben kann – und damit uneingeschränkten Zugang zum «digitalen Binnenmarkt» der EU behält. Das EU-Datenschutzrecht hat folglich einen grossen Einfluss auf die Schweiz. Das schweizerische Datenschutzrecht wurde zudem soeben totalrevidiert. Im vorliegenden Bericht wird die Vereinbarkeit des *CLOUD Acts* mit dem

¹⁵⁸ DASKAL, SWIRE, «The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards».

geltenden und dem künftigen Datenschutzrecht analysiert. Das Ergebnis dieser Analyse legt den Schluss nahe, dass eine Herausgabe von Daten gestützt auf eine Herausgabeanordnung auf der Grundlage des *CLOUD Acts* nur in spezifischen Ausnahmefällen mit dem schweizerischen und europäischen Datenschutzrecht vereinbar ist.

- Rechtshilferecht: Der *CLOUD Act* ermöglicht die Übermittlung elektronischer Daten von einem CSP im Ausland an eine US-Strafverfolgungsbehörde, welche die erhaltenen Daten und Informationen in der Folge in einem US-Strafverfahren als Beweismittel verwenden darf. Diese direkte Zusammenarbeit würde den herkömmlichen Rechtshilfeweg mindestens teilweise ersetzen. Der Abschluss eines *Executive Agreements* würde damit zu einem *Paradigmenwechsel* im Bereich der internationalen Strafrechtskooperation führen: Erstmals würde ein schweizerischer Privater direkt an einem ausländischen Strafverfahren mitwirken, ohne dass dafür ein schweizerisches Verfahren oder wenigstens eine Bewilligung im Einzelfall vorliegt. Diese neue Form der Zusammenarbeit hätte Auswirkungen auf verschiedene Garantien und Prinzipien, welche im Recht der internationalen Rechtshilfe in Strafsachen gelten. Insbesondere betroffen wären die verfassungsmässigen Garantien des rechtlichen Gehörs und des Zugangs zu einem Gericht in der Schweiz, da die von der Datenherausgabe betroffene Person (Datenherr/in) keine Kenntnis von der Bekanntgabe mehr erlangen würde und dagegen folglich auch keine Beschwerde erheben könnte. Auch könnte das BJ seine Rolle als Aufsichtsbehörde im Rechtshilfeverfahren und damit als Garant der Einhaltung der einschlägigen schweizerischen Rechtsprinzipien nicht mehr wahrnehmen. Die Herausgabe wäre einzig abhängig vom Kooperationswillen des CSP. So würden die Rechte der von einem Rechtshilfeersuchen betroffenen Personen geschwächt, aber auch die Möglichkeiten staatlicher Kontrolle – und damit letztlich die schweizerische Souveränität über das Verfahren. Auch mit Blick auf die Vereinbarkeit mit den Prinzipien des Rechtshilferechts wirft der *CLOUD Act* also grosse Fragen auf und scheint schwer mit dem übergeordneten schweizerischen Recht vereinbar zu sein.

8 Weiteres Vorgehen

Der vorliegende Bericht soll eine *Grundlage zur Diskussion* mit Partnerdiensten inner- und ausserhalb der Bundesverwaltung sowie mit Stakeholdern aus Verbänden, der Privatwirtschaft sowie weiteren interessierten Kreisen bilden. Gestützt auf die Ergebnisse aus dieser Diskussion wird das BJ zu gegebener Zeit Antrag an das GS EJPD bezüglich weiterem Vorgehen in Sachen US *CLOUD Act* im Speziellen und «E-Evidence» generell stellen.

9 Bibliographie

- BAERISWYL, B., «Vorbemerkungen zu Art. 4–11a» in Baeriswyl, B. (Hrsg.), *Datenschutzgesetz – Stämpfli Handkommentar*, Bern: Stämpfli 2015.
- BAERISWYL, B., «Art. 4», in Baeriswyl, B. (Hrsg.), *Datenschutzgesetz – Stämpfli Handkommentar*, Bern: Stämpfli 2015.
- BAERISWYL, B., «Art. 10a», in Baeriswyl, B. (Hrsg.), *Datenschutzgesetz – Stämpfli Handkommentar*, Bern: Stämpfli 2015.
- BAERISWYL, B., BLONSKI, D., «Art. 6», in Baeriswyl, B. (Hrsg.), *Datenschutzgesetz – Stämpfli Handkommentar*, Bern: Stämpfli 2015.
- BILGIC, S., «Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act», 32:1 2018 *Harvard Journal of Law and Technology*, S. 321.
- BISMUTH, R., «Le Cloud Act face au projet européen E-Evidence: confrontation ou coopération?», in *Revue critique de droit international privé*, 2019:3, S. 681.
- CHRISTAKIS, T., «21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)», *European Law Blog*, 17.10.2019, abrufbar unter: <https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/>.
- DASKAL, J., «Unpacking the CLOUD Act», 2018:4 *eucrim*, S. 220.
- DASKAL, J., «Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0», 2018:71 *Stanford Law Review Online* S. 9, abrufbar unter: [Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0 | Stanford Law Review](#).
- DASKAL, J., SWIRE, P., «The UK-US CLOUD Act Agreement is Finally Here, Containing New Safeguards», *Just Security*, 08.10.2019, abrufbar unter: <https://www.justsecurity.org/66507/the-uk-us-cloud-act-agreement-is-finally-here-containing-new-safeguards/>.
- DASKAL, J., SWIRE, P., CHRISTAKIS, T., «The globalization of criminal evidence», 16.10.2018, abrufbar unter: <https://iapp.org/news/a/the-globalization-of-criminal-evidence/>.
- LUTZ T., EGLI L., «Braucht die Schweiz ein CLOUD Act Executive Agreement?», *Schweizerische Juristen-Zeitung* SJZ 2021, S. 119.
- MAURER-LAMBROU, U., STEINER, A., «Art. 6 DSG», in Maurer-Lambrou, U., Blechta, G.P. (Hrsg.), *Basler Kommentar: Datenschutzgesetz – Öffentlichkeitsgesetz*, Basel: Helbing Lichtenhahn 2014.
- MAURER-LAMBROU, U., STEINER, A., «Art. 4 DSG», in Maurer-Lambrou, U., Blechta, G.P. (Hrsg.), *Basler Kommentar: Datenschutzgesetz – Öffentlichkeitsgesetz*, Basel: Helbing Lichtenhahn 2014.
- PLENACOSTE, F., DAOUD, E., «CLOUD Act: Des inquiétudes légitimes», 2018:12 *Droit de la propriété intellectuelle et du numérique*, S. 680.

Bericht zum US Cloud Act

RAMPINI, C., «ART. 13 DSGVO», in Maurer-Lambrou, U., Blechta, G.P. (Hrsg.), *Basler Kommentar: Datenschutzgesetz – Öffentlichkeitsgesetz*, Basel: Helbing Lichtenhahn 2014.

ROSENTHAL, D., JÖHRI, Y., *Handkommentar zum Datenschutzgesetz*, Zürich: Schulthess 2008.

ROSENTHAL, D., «Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act», *Jusletter*, 10. August 2020.

TSILIKIS, D., «Auf der grenzüberschreitenden Suche nach E-Evidence im Strafverfahren: die Unionsrechtsperspektive im digitalen Zeitalter», in Meier, J., Zurkinden, N., Staffler, L. (Hrsg.), *Recht und Innovation – Innovation durch Recht, im Recht und als Herausforderung für das Recht*, Zürich: Dike 2020, S. 163.

ZAGARIS, B., «U.S. and UK Sign Cross-Border Data Access Agreement for Cross-Border Enforcement and Warn Facebook on Proposed Encryption», 35:10 2019 *International Enforcement Law Reporter*, S. 357.

ZERDICK, T., «Art. 48 – Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung» in Ehmann, E., Selmayr, M. (Hrsg.), *Datenschutz-Grundverordnung – Kommentar*, 2. Aufl., Beck: München 2018.

ZIMMERMANN, R., *La coopération judiciaire internationale en matière pénale*, 5. Aufl., Bern: Stämpfli 2019.

EDPB/CEPD, «Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence», 10. Juli 2019, abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf (EDPB/CEPD, Initial legal assessment).

US DOJ, «Promoting Public Safety, Privacy, and the Rule of Law around the World: The Purpose and Impact of the CLOUD Act», White Paper, 2019, abrufbar unter: <https://www.justice.gov/dag/page/file/1153436/download>.

10 Abkürzungen

Abs.	Absatz
Art.	Artikel
BBl	Bundesblatt
BG	Bundesgesetz
BG-RVUS	Bundesgesetz zum Staatsvertrag mit den USA über gegenseitige Rechtshilfe in Strafsachen
BJ	Bundesamt für Justiz
BSK	Basler Kommentar
Bst.	Buchstabe(n)
Budapest-Konvention	Übereinkommen des Europarates über die Cyberkriminalität (Cybercrime-Konvention)
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft
CLOUD Act	Clarifying Lawful Overseas Use of Data Act (USA)
CSP	Communication Service Provider
Datenschutzkonvention 108+	Änderungsprotokoll zur Datenschutzkonvention des Europarates
Dienst ÜPF	Dienst Überwachung Post- und Fernmeldeverkehr
DOJ	U.S. Department of Justice
DSG	Bundesgesetz über den Datenschutz
DSGVO	Datenschutz-Grundverordnung der EU
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EEA-Richtlinie	Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen
E-Evidence	Bestrebungen der EU zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
EPOC	Europäische Herausgabeordnung
EPOC-PR	Europäische Sicherungsanordnung
Erw.	Erwägung
EUeR	Europäisches Übereinkommen über die Rechtshilfe in Strafsachen
EuGH	Gerichtshof der EU (Europäischer Gerichtshof)
FDA	Anbieter von Fernmeldediensten
FINMA	Eidgenössische Finanzmarktaufsicht
FMG	Fernmeldegesetz
GS EJPD	Generalsekretariat des Eidgenössischen Justiz- und Polizeidepartements
IRSG	Bundesgesetz über internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz)
IRSV	Verordnung über internationale Rechtshilfe in Strafsachen (Rechtshilfeverordnung)
nDSG	Total revidiertes Datenschutzgesetz vom 25.09.2020
OV-EJPD	Organisationsverordnung für das Eidgenössische Justiz- und Polizeidepartement
QFG	Qualifying foreign government (Staat, der ein Executive Agreement mit den USA abgeschlossen hat)
RVUS	Staatsvertrag Schweiz-USA über gegenseitige Rechtshilfe in Strafsachen
SCA	Stored Communications Act (USA)
SDSG	Bundesgesetz über den Datenschutz in Anwendung des Schengen-Besitzstands in Strafsachen
SEV	Sammlung der Europaratsverträge
SHK	Stämpfli Handkommentar
SR	Systematische Sammlung des Bundesrechts
StIGH	Ständiger Internationaler Gerichtshof (bis 1946)

Bericht zum US Cloud Act

StGB	Schweizerisches Strafgesetzbuch
StPO	Schweizerische Strafprozessordnung
T-CY	Komitee des Europarates für die Cybercrime-Konvention
UK	Vereinigtes Königreich
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VwVG	Bundesgesetz über das Verwaltungsverfahren
WVK	Wiener Vertragsrechtskonvention
Ziff.	Ziffer



17 septembre 2021

Rapport sur le US CLOUD Act (loi *Cloud*)



Table des matières

1	Mandat.....	4
2	Introduction.....	4
3	Le <i>CLOUD Act</i>.....	6
3.1	Contexte.....	6
3.2	Sommaire.....	6
3.2.1	Principal contenu matériel	6
3.2.2	Conclusion possible d' <i>executive agreements</i> avec d'autres États sur la base du <i>CLOUD Act</i>	7
3.2.2.1	Généralités	7
3.2.2.2	Conditions matérielles	8
3.2.2.3	Conditions formelles	8
3.2.3	Contenu de l'accord bilatéral	9
3.2.4	Conditions requises pour les injonctions de production en vertu d'un <i>executive agreement</i>	9
4	Droit comparé	10
4.1	<i>Executive agreement</i> entre les USA et le Royaume-Uni.....	10
4.2	Législation <i>e-evidence</i> de l'UE et US <i>CLOUD Act</i> : conflit ou négociation ?	12
4.2.1	Législation <i>e-evidence</i> de l'UE	12
4.2.2	Discussions entre l'Union européenne et les USA.....	13
4.3	Deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention du Budapest)	15
5	Les questions juridiques.....	16
5.1	Territorialité et souveraineté	16
5.2	Nature des <i>executive agreements</i>	17
5.3	Notion de « <i>serious crime</i> » (infraction grave)	19
5.4	Collecte de données électroniques.....	20
5.4.1	Destinataires	20
5.4.2	Type de données.....	21
5.4.3	Modalités de collecte	22
5.5	Protection des droits fondamentaux, en particulier protection des données et de la vie privée	23
5.5.1	Niveau européen : lien entre le <i>CLOUD Act</i> et le règlement général de l'UE sur la protection des données (RGPD)	23
5.5.1.1	Compatibilité du <i>CLOUD Act</i> et du RGPD	23
5.5.1.2	Bilan : risques liés à la conclusion d'un <i>executive agreement</i> avec les USA pour la décision d'adéquation de la Suisse	26
5.5.2	Licéité du traitement des données et des divulgations fondées sur une injonction de production basée sur le <i>CLOUD Act</i> sous l'angle du droit suisse.	29
5.5.2.1	Aspects pertinents du cadre juridique de la protection des données en Suisse	29
5.5.2.2	Aspects problématiques au regard des principes de la protection des données en Suisse	30
5.5.2.3	Motifs justificatifs pour les personnes physiques en cas d'atteinte à la personnalité, art. 13 LPD/art. 27 nLPD	32

Rapport sur le US CLOUD Act (loi *Cloud*)

5.5.2.4	Compatibilité avec les exigences relatives à la communication transfrontière de données (art. 6 LPD/art. 16 et 17 nLPD)	34
5.5.2.5	Autres aspects problématiques du point de vue de la protection des données et de la protection des droits fondamentaux	34
5.5.2.6	Conclusion sur la compatibilité d'un <i>executive agreement</i> avec la protection des données	35
5.5.3	Quelle protection devrait être incluse dans un <i>executive agreement</i> avec les USA ?	36
5.6	Compatibilité avec le droit suisse d'entraide judiciaire	37
5.6.1	Motifs de refus d'une requête d'entraide judiciaire et garantie de recours judiciaire	38
5.6.2	Principe de la double incrimination	39
5.6.3	Droit d'être entendu	39
5.6.4	Autorité de surveillance et de contrôle	40
5.6.5	Principe de spécialité	41
5.6.6	Limitation de la coopération internationale pour motifs politiques	42
5.6.7	Compatibilité avec le code de procédure pénale et la loi fédérale sur la surveillance de la correspondance par poste et télécommunication	43
5.6.8	Quels contenus « juridiques d'entraide judiciaire » devraient figurer dans un <i>executive agreement</i> ?	44
6	Sécurité des données et décryptage	44
6.1	Transmission sécurisée	44
6.2	Cryptage neutre	45
7	Conclusion	46
8	Procédure à suivre	47
9	Bibliographie	48
10	Abréviations	50

1 Mandat

En mars 2018, les USA ont adopté le *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*¹. Dans le domaine de la prévention, de la détection, des enquêtes et des poursuites de crimes graves (*serious crimes*), il doit permettre aux autorités de poursuite pénale américaines d'accéder aux données des fournisseurs de services de communication (*Communication Service Providers*, CSPs) ayant leur siège aux USA, que ces données soient stockées aux USA ou à l'étranger, p. ex. via des filiales, conférant ainsi à la loi américaine un effet extraterritorial². Dans certaines conditions, le *CLOUD Act* permet aux USA de conclure des accords d'exécution bilatéraux (*executive agreements*) avec d'autres États. Ainsi, les autorités de poursuite pénale de l'État partenaire peuvent envoyer des requêtes directement aux CSPs se trouvant aux USA et réciproquement. Pour cela, l'État partenaire doit accepter que les autorités de poursuite pénale américaines accèdent aux données enregistrées par les CSPs ayant leur siège sur son territoire. C'est surtout cet aspect qui incite à se demander dans quelle mesure la conclusion d'un tel accord avec les USA serait opportun pour la Suisse.

En Suisse, l'Office fédéral de la justice (OFJ) est l'organe central dans le domaine de la coopération pénale internationale³. À ce titre, il surveille l'application de la loi sur l'entraide internationale en matière pénale (EIMP)⁴ et il est en plus responsable du développement des bases légales dans ce domaine. Il a élaboré le présent rapport suite à l'intervention dans ce contexte de différents acteurs de l'économie privée, des associations professionnelles, de l'administration et des autorités de poursuite pénale. Ce document permettra d'approfondir la discussion avec les parties prenantes publiques et privées en Suisse. À cet effet, il apporte notamment des éclaircissements sur les questions juridiques fondamentales qui se posent en termes de compatibilité entre le *CLOUD Act* et le droit suisse.

2 Introduction

Au vu du phénomène de mondialisation, la coopération pénale internationale joue un rôle de plus en plus important. Avec la digitalisation croissante de tous les aspects de la vie, et dans le présent contexte, la collecte et la transmission de preuves électroniques, cette coopération fait face à des défis de nature très différente :

- Les données sont *volatiles* – l'entraide pénale traditionnelle est souvent trop lente pour garantir leur sécurité en temps opportun et au-delà des frontières nationales ;
- Les données n'ont pas de *marquage territorial* – le *lieu de stockage* doit-il vraiment être déterminant pour l'accès des autorités de poursuite pénale aux données ou bien la question n'est-elle pas plutôt de savoir qui peut y avoir accès et depuis quel endroit ? Le problème est encore plus complexe pour les *blockchains* car les données ne sont pas stockées physiquement dans un lieu clairement défini ;
- Les données sont *cryptées* – comment peuvent-elles être décryptées efficacement par les autorités de poursuite pénale dans le trafic international des données ? Existe-t-il des règles internationales ou globales ?

Une chose est sûre : la collecte internationale de preuves électroniques remet en question les fondements de la coopération pénale internationale. Elle bouleverse le sens actuel du principe de territorialité. Les procédures d'entraide pénale traditionnelle basée sur la notion de

¹ Texte complet disponible sur : <https://www.congress.gov/bills/115th-congress/senate-bill/2383/text>.

² Il faut d'ores et déjà souligner que le *CLOUD Act* s'applique uniquement dans le cadre de *procédures pénales*. Dans ce type de procédure, le principe de territorialité revêt une importance particulière pour diverses raisons. Cf. paragraphes 2. et 5.1 ci-dessous. Par la suite, il sera donc question de *Territorialité au vu du droit pénal*.

³ Cf. art. 17 Loi sur l'entraide pénale internationale (EIMP, RS 351.1) et art. 3 Ordonnance sur l'entraide pénale internationale (OEIMP, RS 351.11).

⁴ RS 351.1.

Rapport sur le US CLOUD Act (loi *Cloud*)

souveraineté sont trop lentes. L'accent est mis sur des formes de collaboration plus directes, et parfois sur la participation expresse de particuliers à des procédures pénales à l'étranger. Cela est en partie nécessaire : les capacités des autorités d'entraide judiciaire des États dans lesquels de nombreux CSPs ont leur siège ont atteint leurs limites.

Actuellement, les éventuelles modifications du droit concernant l'entraide judiciaire font l'objet de discussions dans différents forums et au sein de l'UE ainsi qu'au Conseil de l'Europe et à l'ONU.

Grâce à sa proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale d'avril 2018 (règlement *e-evidence*)⁵, l'UE souhaite faciliter et accélérer la collaboration entre ses États membres. Au sein du Conseil de l'Europe, le Comité de la Convention sur la cybercriminalité (T-CY), qui représente les États parties à la Convention de Budapest⁶, élabore actuellement un deuxième protocole pour cette convention, qui est censé régler de manière générale la collaboration internationale pour les crimes commis au moyen de systèmes informatiques et pour les preuves électroniques. De son côté, l'ONU prépare un instrument multilatéral pour lutter contre la cybercriminalité.

Alors que des instruments multilatéraux censés favoriser la collaboration entre les États font l'objet de discussions dans ces forums, les USA ont, avec le *CLOUD Act*, adopté en mars 2018 au niveau national, une loi dont la portée est extraterritoriale. D'une part, cette loi doit permettre aux autorités de poursuite pénale américaines d'accéder aux données des CSPs dont le siège est aux USA, que ces données soient enregistrées aux USA ou à l'étranger, sans avoir à engager une procédure par la voie de l'entraide judiciaire internationale. D'autre part, elle doit d'autre part permettre aux États étrangers concernés d'avoir également accès aux données des CSPs ayant leur siège aux USA, sans avoir à déposer une requête d'entraide judiciaire, grâce aux accords d'exécution bilatéraux. Il leur suffit pour cela d'envoyer leurs requêtes directement aux CSPs concernés. Cependant, ces États étrangers ne peuvent pas contraindre les CSPs à donner suite à leurs requêtes. L'*executive agreement* permet certes aux CSPs de fournir des données à un État étranger, mais ils n'y sont pas obligés.

La Suisse a conclu un accord d'entraide judiciaire avec les USA dans le cadre du traité du 25 mai 1973 entre la Confédération Suisse et les États-Unis d'Amérique sur l'entraide judiciaire en matière pénale ((TEJUS)⁷. Par conséquent, les autorités suisses ont accès aux données des CSPs américains via l'entraide pénale internationale. Cependant, cette procédure est longue car le Département américain de la justice (DOJ) doit examiner la requête correspondante avant de la transmettre à l'autorité d'exécution, qui en général ne peut la satisfaire qu'après une procédure judiciaire, à l'issue de laquelle elle est finalement autorisée à transmettre les moyens de preuve. L'expérience des autorités de poursuite pénale suisses en la matière révèle que les preuves électroniques demandées ne sont pas toujours transmises, ou du moins pas toujours transmises à temps. En 2016, le DOJ a déjà édicté des directives concernant les preuves électroniques afin d'exhorter les autorités étrangères à s'adresser directement aux CSPs, lorsqu'elles souhaitent uniquement avoir accès aux données personnelles des abonnés (*basic subscriber information* : nom et adresse, type et durée du service fourni,

⁵ Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, COM/2018/225 final – 2018/0108 (COD) du 17 avril 2018.

⁶ Convention du Conseil de l'Europe sur la cybercriminalité, STE 185, RS 0.311.43.

⁷ RS 0.351.933.6.

Rapport sur le US CLOUD Act (loi *Cloud*)

moyens de paiement y c. numéros de carte de crédit et de compte ; « données personnelles »)⁸. En pratique, certains CSPs fournissent déjà ce type de données tandis que d'autres refusent de le faire et renvoient à la procédure officielle.

Même si la Suisse concluait un *executive agreement* avec les USA, la situation demeurerait inchangée. En outre, la mise en œuvre de mesures de contrainte ne pourrait être demandée que par la voie de l'entraide judiciaire et cette contrainte pourrait être exercée uniquement par l'intermédiaire de l'autre État. Après la conclusion d'un *executive agreement*, les autorités de poursuite pénale suisses pourraient s'adresser directement à un CSP, également pour des données encore plus sensibles que les données personnelles, mais elles ne seraient pas autorisées à ordonner la mise en œuvre de mesures de contrainte. Si un CSP refusait de lui donner accès à des données, la Suisse devrait engager une procédure d'entraide judiciaire pour les demander et les collecter via des mesures de contrainte. Mais si un CSP acceptait, la collaboration serait plus efficace. Dans ce cas-ci, elle permettrait de délester l'entraide judiciaire avec les USA de sorte que les autorités impliquées pourraient se concentrer sur des cas, pour lesquels les CSPs refusent de coopérer ou qui n'entrent pas dans le champ d'application du *CLOUD Act*. On suppose que les CSPs qui acceptent déjà de coopérer continueront de produire des données personnelles en raison de la clarification de la situation juridique et en s'appuyant sur un *executive agreement*. Les autres CSPs seraient éventuellement intéressés par ce type de collaboration.

3 Le *CLOUD Act*

3.1 Contexte

Le *CLOUD Act* est une loi fédérale américaine qui complète la loi sur les communications enregistrées, le *Stored Communications Act* (SCA), et qui a été promulguée en mars 2018 dans le cadre d'une procédure judiciaire impliquant Microsoft. En 2013, la société Microsoft avait été sommée par un juge américain de communiquer des e-mails et des informations sur un compte hébergé par Microsoft en vertu du SCA. L'entreprise avait communiqué les informations qui se trouvaient sur un serveur hébergé aux USA, mais avait refusé de transmettre les e-mails qui étaient stockés sur un serveur en Irlande. Elle avait argué qu'une entreprise américaine ne pouvait être tenue, sur la base d'une telle injonction, de communiquer des données stockées sur un serveur hébergé à l'étranger. Selon Microsoft, le tribunal américain n'avait aucune compétence en la matière, le SCA n'ayant pas d'effet extraterritorial.

Microsoft a perdu le procès en première instance, mais la Cour d'appel lui a donné raison. Le Département américain de la justice a fait appel de cette décision devant la Cour suprême. Avant même que le jugement ne soit rendu, le Congrès a adopté le *CLOUD Act* qui modifie le SCA et qui confère à la loi son effet extraterritorial actuel.

3.2 Sommaire

3.2.1 Principal contenu matériel

Le *CLOUD Act* oblige les CSPs dont le siège est aux USA et qui gèrent des centres de stockage de données hors des USA, de conserver les données hébergées sur leurs serveurs et de les communiquer sur demande aux autorités judiciaires américaines. Cette loi s'applique in-

⁸ Selon la législation actuelle, la demande d'accès aux données personnelles des abonnés doit s'effectuer dans tous les cas par la voie de l'entraide judiciaire.

Rapport sur le US CLOUD Act (loi *Cloud*)

dépendamment du lieu d'enregistrement de ces données, que ce soit aux USA ou à l'étranger⁹. Sont concernées les sociétés de droit américain, c'est-à-dire celles qui sont soumises à la juridiction américaine¹⁰. Dans ce cadre, des contacts minimaux (*minimum contacts*) avec les USA sont une condition nécessaire ; l'interprétation et la qualification de ces contacts relèvent toutefois de la compétence des tribunaux américains. Les entreprises détenant des holdings, filiales ou succursales aux USA peuvent également être concernées, tout comme des prestataires étrangers qui font de la publicité pour leurs services de cloud aux USA. Seuls les CSPs étrangers qui n'entretiennent pas ces contacts minimaux avec les USA ne sont pas soumis à de nouvelles obligations.

Le *CLOUD Act* ne stipule aucune durée minimale pour la conservation des données. Toutefois, si l'on se réfère à d'autres dispositions du droit américain, par exemple le SCA, il semble – au moins dans certains cas – qu'une obligation de conserver les données pendant 180 jours s'applique.

En vertu du *CLOUD Act*, le CSP peut contester devant un tribunal américain une injonction des autorités de poursuite pénale concernant la divulgation de données (une motion en modification ou en annulation), si la personne concernée n'est pas une *US person*¹¹ et si la divulgation des données risque de violer le droit d'un État ayant conclu un *executive agreement* (cf. point 3.2.2 ci-dessous) avec les USA (gouvernement étranger qualifié ou *qualifying foreign government* ; QFG). Pour sa décision concernant l'annulation ou la modification de l'injonction de production des données qui est contestée, le tribunal tient compte des intérêts des USA ou du QFG, des relations entre la personne concernée et, d'une part, les USA et, d'autre part, l'État qui a demandé la divulgation des données, de la probabilité d'une sanction et son éventuelle sévérité, de l'importance des données demandées pour l'enquête, des intérêts des autorités requérantes ainsi que de la probabilité d'accéder opportunément et efficacement aux données correspondantes via des possibilités moins radicales¹². Si le tribunal le juge nécessaire, la divulgation immédiate des données peut être ordonnée avant même que la décision portant sur une motion en modification ou en annulation n'ait été prise¹³.

Ni l'État étranger, ni la personne concernée ne peuvent s'opposer à la requête des autorités américaines. Seul le CSP est en mesure de le faire.

3.2.2 Conclusion possible d'*executive agreements* avec d'autres États sur la base du *CLOUD Act*

3.2.2.1 Généralités

La deuxième partie du *CLOUD Act* permet aux USA de conclure dans certaines conditions des *executive agreements* avec d'autres États. En vertu de ces accords bilatéraux, les autorités compétentes des deux États peuvent demander directement aux CSPs, dont le siège se trouve dans l'un ou l'autre État partie à l'accord, de leur divulguer des informations ou des données stockées sur leurs serveurs. Sur la base d'*executive agreements*, les CSPs peuvent donner directement suite à l'injonction de production internationale (*international production order*, « injonction de production ») envoyée directement par l'autre État. Comme indiqué, les

⁹ *CLOUD Act*, §2713. Cf. également BISMUTH, p. 683.

¹⁰ DOJ, « Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act », p. 6 ss

¹¹ *CLOUD Act*, § 2713 (h) (2) (A)

¹² *CLOUD Act*, § 2713 (h) (3) (A)

¹³ *CLOUD Act*, § 2713 (h) (4)

Rapport sur le US CLOUD Act (loi *Cloud*)

CSPs ne peuvent être contraints par l'État étranger de divulguer des données. Une injonction de production ne se substitue donc pas à l'entraide judiciaire, tout du moins lorsque le CSP ne coopère pas de manière volontaire.

3.2.2.2 Conditions matérielles

Selon le *CLOUD Act*, l'État qui souhaite négocier un *executive agreement* avec les USA doit remplir certaines conditions minimales¹⁴ :

La législation nationale de l'État concerné doit offrir de « solides » garanties matérielles et procédurales, comparables à celles des USA, pour protéger la sphère privée et les libertés civiles eu égard à la collecte des données et à ses activités entrant dans le cadre des *executive agreements*. Il doit en effet garantir des dispositions légales adaptées en matière de cybercriminalité et de preuves électroniques. L'État concerné peut notamment en apporter la preuve en faisant valoir son adhésion à la Convention de Budapest.

De manière générale, l'État concerné doit veiller au respect de l'État de droit et du principe de non-discrimination. Il doit en outre se conformer aux obligations internationales en vigueur en matière de droits humains, parmi lesquelles la protection contre les immixtions arbitraires et illégales dans la sphère privée, le droit à une procédure équitable et à la liberté d'expression, d'association et de réunion, l'interdiction des arrestations et détentions arbitraires ainsi que de la torture et des traitements cruels, inhumains ou dégradants.

Les services gouvernementaux qui sont en droit de demander la divulgation de données en vertu des *executive agreements* doivent avoir un mandat clairement défini sur le plan juridique. Ils doivent en outre disposer de directives et de procédures claires concernant la collecte, l'enregistrement, l'utilisation et la divulgation des données. Des mécanismes suffisants, avec lesquels le gouvernement étranger peut prouver la transparence concernant la collecte et la saisie de données électroniques, doivent être disponibles.

L'État concerné doit apporter la preuve qu'il s'efforce d'encourager et de protéger la libre circulation de l'information dans le monde et de promouvoir le caractère ouvert, libre et interconnecté de l'Internet¹⁵. Enfin, il doit garantir des droits réciproques pour l'accès aux données. Cela signifie qu'il doit autoriser les CSPs siégeant sur son territoire à répondre directement aux requêtes des autorités de poursuite pénale américaines.

Une injonction de production reposant sur l'*executive agreement* ne doit pas viser directement des citoyens américains ou *US persons*. L'État concerné doit donc prendre des mesures appropriées pour éviter une telle situation. Le *CLOUD Act* contient la liste complète des autres conditions que doit remplir une injonction de production¹⁶.

3.2.2.3 Conditions formelles

Aux USA, la conclusion des *executive agreements* relève des compétences de l'exécutif. Le procureur général des USA (US Attorney General) décide avec le Ministre des Affaires étrangères si l'autre État remplit les conditions nécessaires à la conclusion de l'accord bilatéral et transmet la confirmation écrite au Congrès américain¹⁷. L'*executive agreement* certifié de

¹⁴ *CLOUD Act*, § 2523 (b)

¹⁵ *CLOUD Act*, §2523 (b) (1) (B) (vi)

¹⁶ *CLOUD Act*, § 2523 (b) (2) et (3)

¹⁷ *CLOUD Act*, §2523 (b)

Rapport sur le US CLOUD Act (loi *Cloud*)

la sorte peut entrer en vigueur aux USA si le Congrès ne formule pas de recours dans un délai de 180 jours¹⁸.

L'accord est conclu pour une durée déterminée. L'État qui conclut un tel accord avec les USA doit dès lors se soumettre à une évaluation périodique par les autorités américaines¹⁹.

3.2.3 Contenu de l'accord bilatéral

La première partie de l'*executive agreement* doit contenir des dispositions à caractère général telles que des définitions, le droit applicable, la forme et le contenu des requêtes, les autorités compétentes et des dispositions relatives à la protection des données.

L'une des principales définitions est celle du *serious crime* (infraction grave). En vertu du *CLOUD Act*, les requêtes fondées sur un *executive agreement* doivent se limiter aux enquêtes pénales portant sur des infractions graves. Outre les actes de terrorisme, explicitement mentionnés dans le *CLOUD Act*, ces infractions concernent notamment les meurtres et les enlèvements d'enfants. Il convient aussi de déterminer les données pouvant être prises en compte dans l'*executive agreement*, à savoir exclusivement les données déjà enregistrées ou également les données collectées en temps réel. Le concept de CSP, avec ce qu'il englobe précisément, doit également être défini.

En Suisse, la collaboration en matière d'entraide judiciaire se heurte à différentes limites. Si l'on considère que le *CLOUD Act* permet une forme de collaboration internationale dans des affaires pénales, il serait judicieux de vérifier, dans le cas de la négociation éventuelle d'un *executive agreement*, dans quelle mesure les principes essentiels du droit suisse sont intégrés dans le texte en vue d'une collaboration. Les éventuels motifs d'irrecevabilité devraient y être négociés et intégrés de manière explicite.

Par conséquent, un éventuel *executive agreement* doit également comporter des dispositions techniques relatives à la transmission d'informations et à l'enregistrement de données. L'accord doit stipuler que la transmission des données et des informations doit se faire via un canal sûr. Il doit également préciser les exigences relatives à l'enregistrement de données dans un système sécurisé et à l'accès à ces données dans l'État requérant.

Sur le plan formel, l'*executive agreement* doit comporter des dispositions concernant les procédures à respecter, notamment sur la question des objections ou des motions en annulation portant sur des injonctions de production.

3.2.4 Conditions requises pour les injonctions de production en vertu d'un *executive agreement*

Conformément au *CLOUD Act*, les injonctions de production fondées sur un *executive agreement* doivent remplir différentes conditions minimales²⁰.

La personne dont les données sont concernées par une injonction de production émanant de l'étranger ne doit pas être une *US person*, c'est-à-dire qu'elle ne doit ni être citoyenne américaine, ni résider aux USA. Dans le cas d'une entreprise, elle ne doit pas avoir son siège aux USA²¹. À l'inverse, les autorités de poursuite pénale américaines n'auraient pas le droit

¹⁸ *CLOUD Act*, §2523(d) (2)

¹⁹ *CLOUD Act*, §2523(b) (4) (J)

²⁰ *CLOUD Act*, § 2523 (b) (3)

²¹ Selon *CLOUD Act*, § 2523 (a) (2) « incorporated in the United States ».

Rapport sur le US CLOUD Act (loi *Cloud*)

d'exiger la divulgation de données de personnes de nationalité suisse, de personnes résidant en Suisse ou d'une société dont le siège est en Suisse, pour autant que ce point soit précisé dans l'accord. Dans le cadre de l'*executive agreement*, l'État étranger n'a pas le droit d'envoyer des injonctions qui visent directement une *US person* ni d'ailleurs des injonctions qui concernent certes une *non US person*, mais qui ont pour but de collecter des informations sur une *US person* et inversement²². Le traitement qui serait réservé aux filiales d'entreprises suisses fondées selon le droit américain n'est pas clair dans ce contexte. Lorsqu'il s'agit de personnes qui sont exclues du domaine d'application de l'*executive agreement*, il convient de demander les données correspondantes dans le cadre de l'entraide judiciaire.

L'injonction de production doit concerner un *serious crime*, une notion à définir dans l'*executive agreement* (cf. point 5.3). En outre, en conformité avec la législation de l'État à l'origine de l'injonction, elle doit indiquer une personne, une adresse, un objet personnel ou une autre caractéristique d'identification et être justifiée par des faits compréhensibles et crédibles (pas de *fishing expeditions*). En outre, elle doit pouvoir être vérifiée par un tribunal ou une autorité indépendante et dans le cas des injonctions de mise sur écoute, elle doit être limitée dans le temps et proportionnelle²³.

L'injonction ne doit pas apporter la preuve qu'il existe une *probable cause*²⁴, ce qui faciliterait la collaboration avec les USA et délésterait considérablement les autorités de poursuite pénale suisses.

4 Droit comparé

4.1 *Executive agreement* entre les USA et le Royaume-Uni

Le Royaume-Uni (RU) est le premier, et à ce jour le seul État avec lequel les USA ont négocié un *executive agreement* en vertu du *CLOUD Act*. Le contenu précis de l'accord signé le 3 octobre 2019, mais qui n'est pas encore entré en vigueur, est disponible en ligne²⁵. Ce premier accord revêt une importance particulière car il devrait également définir les grandes lignes des futurs *executive agreements*.

Il s'agit d'un accord relativement court dont plusieurs des points renvoient à d'autres accords, à savoir la Convention de Budapest, l'accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel²⁶ et l'accord d'entraide judiciaire en matière pénale conclu entre les USA et le Royaume-Uni. De par sa structure, cet accord est comparable à un accord d'entraide judiciaire en matière pénale. Il contient des définitions, une finalité, des limites, des dispositions sur la protection des données, etc.

Parmi les notions importantes définies dans le cadre de l'*executive agreement* figurent notamment les autorités compétentes, le CSP, les données et le *serious crime* (Art. 1). Les injonctions de divulgation ou de production de données enregistrées hors de l'État (« injonction ») doivent être conformes au droit national de la partie requérante (art. 5, al. 1). En revanche, le droit national de la partie dans laquelle se trouve le CSP ne doit pas forcément être respecté. L'injonction doit pouvoir être portée devant une autorité judiciaire ou une

²² *CLOUD Act*, § 2523 (b) (3) (A) et (B)

²³ *CLOUD Act*, § 2523 (b) (3) (D)

²⁴ DOJ, « Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act », p. 8.

²⁵ Contenu disponible sur : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf. D'après les informations de l'Ambassade britannique à Berne, l'accord devrait entrer en vigueur à la fin de l'été 2021.

²⁶ Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, JO L 336 du 10 décembre 2016, p. 3.

Rapport sur le US CLOUD Act (loi *Cloud*)

autorité indépendante de la partie requérante afin que ces autorités puissent vérifier que l'injonction est compatible avec la législation nationale (art. 5, al. 2). Cela signifie qu'un CSP dont le siège est aux USA et qui reçoit une injonction du Royaume-Uni peut porter l'affaire devant les autorités britanniques. Pour les petits CSPs, il peut s'avérer difficile d'intenter une action en justice dans un autre pays, en particulier aux USA. L'*executive agreement* prévoit donc une sorte d'autorité centrale qui doit contrôler la conformité de l'injonction avec l'accord, avant qu'elle ne soit envoyée au CSP (Art. 5, al. 6). Selon cette disposition, une autorité souhaitant collecter des informations auprès d'un CSP doit d'abord consulter cette autorité centrale.

Si un CSP considère que l'injonction reçue n'est pas conforme à l'accord, il doit d'abord l'invoquer auprès des autorités désignées de l'État qui transmet l'injonction, soit l'État dans lequel il n'est pas incorporé. En cas de désaccord subsistant, il peut alors également s'adresser aux autorités désignées dans l'État dans lequel il est incorporé (art. 5, al. 11). Les deux autorités s'efforcent de trouver une solution consensuelle. Si l'État « requis » considère que l'injonction n'est pas conforme à l'accord, il peut en informer l'autorité de la partie « requérante » et l'accord ne sera pas applicable à l'injonction (art. 5, al. 12). Il semblerait donc qu'il y ait une procédure selon laquelle l'autorité centrale de l'État de résidence peut décider en dernière instance si une injonction est conforme ou non à l'*executive agreement*.

Les données obtenues sur la base de l'accord ne peuvent être transmises à un État tiers sans le consentement de l'État dans lequel le CSP est incorporé (Art. 8, al. 2). Si la personne dont les informations sont demandées ne se trouve pas sur le territoire de l'État « requérant » et si elle n'est pas citoyenne de cet État, l'État tiers dont elle est ressortissante doit en être informé²⁷.

Si les données concernent des cas qui pourraient mener à la prononciation d'une peine de mort aux USA ou à la violation de la liberté d'expression au Royaume-Uni, l'autorité centrale de l'autre État doit être impliquée et donner son accord (art. 8, al. 4). Sans l'accord de l'autre État, les données obtenues sur la base du *CLOUD Act* au Royaume-Uni ne peuvent être utilisées pour prononcer une peine de mort aux USA et les données obtenues aux USA ne peuvent servir à prononcer une sanction liée à une violation de la liberté d'expression au Royaume-Uni²⁸. Il existe donc des droits de veto correspondants²⁹.

En ce qui concerne les personnes visées par l'*executive agreement*, il y a une asymétrie entre les USA et le Royaume-Uni. En effet, les injonctions britanniques ne peuvent pas viser des *US persons*. Cela inclut à la fois les personnes qui résident aux USA, quelle que soit leur nationalité, et les citoyens américains qui résident à l'étranger. À l'inverse, les injonctions américaines peuvent en principe viser des citoyens britanniques. Les personnes qui ne sont pas de nationalité anglaise, mais qui résident *sur le territoire britannique* sont exclues du champ d'application de l'accord. Cette disposition semble s'appuyer sur les principes du droit de l'UE (citoyenneté européenne)³⁰.

Dans le cadre de l'*executive agreement*, les CSPs ne sont pas tenus de se conformer aux requêtes provenant des autorités de l'autre État. Si un CSP refuse de répondre, c'est la loi

²⁷ DASKAL, SWIRE, « The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards ». Art. 5 de l'accord.

²⁸ CHRISTAKIS, « 21 Thoughts and Questions about the UK-US *CLOUD Act* Agreement », pt. 15–16 ; Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America in Access to Electronic Data for the Purpose of Countering Serious Crime, pt. 19–20.

²⁹ DASKAL, SWIRE, « The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards ».

³⁰ Contenu disponible sur : <https://www.hrw.org/news/2019/10/29/groups-urge-congress-oppose-us-uk-cloud-act-agreement>.

Rapport sur le US CLOUD Act (loi *Cloud*)

du pays qui émet la requête qui s'applique³¹. Si une mesure de contrainte est nécessaire, il faudra en principe passer par la voie de l'entraide pénale internationale. L'accord est neutre en ce qui concerne le cryptage. Il n'oblige pas les CSPs à supprimer les cryptages³².

Les parties évaluent le respect de l'*executive agreement* un an après son entrée en vigueur, puis de manière périodique (art. 12, al. 1). Chaque partie doit également établir un rapport annuel sur l'application de l'accord qu'elle soumettra à l'autre État (art. 12, al. 4). L'accord s'applique pendant une durée de cinq ans et pourra par la suite être résilié ou prolongé pour une durée indéterminée.

4.2 Législation e-evidence de l'UE et US CLOUD Act : conflit ou négociation ?

4.2.1 Législation e-evidence de l'UE

Des efforts sont actuellement entrepris au niveau de l'UE pour améliorer l'accès transfrontalier aux preuves électroniques (dites *e-evidence*). Un cadre juridique visant à faciliter et à accélérer la sécurisation des preuves électroniques et leur accès transfrontière pour les autorités policières et judiciaires est en cours d'élaboration. L'idée d'une législation sur les preuves électroniques remonte aux attaques terroristes de mars 2016 à Bruxelles et à la demande qui en a résulté dans l'UE de trouver de nouveaux moyens de sécuriser les preuves électroniques plus rapidement et plus efficacement et de coopérer plus étroitement avec les pays tiers et les prestataires de services opérant sur le territoire européen³³.

En avril 2018, la Commission a présenté deux propositions législatives sur les *e-evidence*, à savoir : une proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale³⁴ et une proposition de directive établissant des règles communes relatives à la désignation de représentants légaux aux fins de la collecte de preuves dans le cadre de procédures pénales³⁵.

La proposition de règlement introduit deux nouveaux instruments contraignants pour les autorités concernées, à savoir l'injonction européenne de production (EPOC) et l'injonction européenne de conservation (EPOC-PR). Ces instruments doivent exister en parallèle des instruments juridiques actuels qui facilitent la collecte de preuves sur le territoire d'un autre État membre, tels que la directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale (« directive décision d'enquête européenne »)³⁶.

L'injonction européenne de production doit permettre aux autorités d'utiliser une ordonnance judiciaire pour demander des données numériques stockées par un CSP dans un autre État membre de l'UE et nécessaires comme preuve dans le cadre d'enquêtes et de procédures pénales. Cette idée repose essentiellement sur le fait que chaque CSP souhaitant fournir des services dans l'UE doit désigner un représentant dans l'UE (appelé *legal representative*)

³¹ Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America in Access to Electronic Data for the Purpose of Countering Serious Crime, pt. 18.

³² CHRISTAKIS, « 21 Thoughts and Questions about the UK-US CLOUD Act Agreement », pt. 14 ; DASKAL, SWIRE, « The UK-US CLOUD Act Agreement is Finally Here, Containing New Safeguards ».

³³ Déclaration commune des ministres européens de la justice et de l'intérieur et des représentants des institutions de l'UE du 24 mars 2016 sur les attentats terroristes perpétrés le 22 mars 2016 à Bruxelles, disponible sur : <https://www.consilium.europa.eu/fr/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/>.

³⁴ Proposition de la Commission européenne pour un règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale du 17 avril 2018, COM(2018)225 final.

³⁵ Proposition de la Commission européenne pour une directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale du 17 avril 2019, COM(2018) 226 final.

³⁶ Directive 2014/41/EU du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale, JO L 130 du 1^{er} mai 2014, p. 1.

Rapport sur le US CLOUD Act (loi *Cloud*)

qui a accès aux données de l'ensemble de l'entreprise. La proposition de directive prévoit des règles uniformes pour la désignation de ces représentants. Les autorités (police ou ministère public d'un État membre de l'UE) peuvent ainsi avoir un accès direct à ce représentant pour la notification et l'exécution des injonctions – quel que soit le lieu où ce représentant a son siège dans l'UE. Ici également, le contact n'a donc plus lieu entre les autorités d'un État, mais entre une autorité et une entreprise, c'est-à-dire une entité privée³⁷. Les entreprises concernées doivent transmettre les données dans un délai de quelques jours à quelques heures (10 jours, en cas d'urgence dans les 6 heures).

L'injonction européenne de conservation – tout comme l'injonction européenne de production – est adressée au représentant d'un CSP qui se trouve en dehors du système juridique de l'État membre émetteur de l'injonction. Avec l'injonction de conservation, les CSPs peuvent être contraints de sauvegarder les données en vue d'une demande ultérieure de remise³⁸.

L'affaire est actuellement discutée en trilogie, terme qui désigne le processus de coordination politique entre la Commission européenne, le Conseil de l'UE et le Parlement européen.

4.2.2 Discussions entre l'Union européenne et les USA

En février 2019, la Commission européenne a sollicité un mandat pour l'ouverture de négociations en vue d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale³⁹. En juin 2019, le Conseil de l'Union européenne a autorisé la Commission à entamer des négociations au nom de l'UE⁴⁰.

L'ouverture de discussions avec les USA s'explique principalement par la législation de l'UE sur les preuves électroniques. Bien que les propositions relatives aux preuves électroniques concernent les CSPs qui fournissent des services sur le marché de l'UE, il y a un risque de conflit entre les obligations prévues dans ces propositions et les dispositions légales d'États tiers. Certes, les projets concernant la législation sur les preuves électroniques de l'UE contiennent des dispositions régissant les conflits de lois. Cependant, étant donné que les principaux CSPs visés dans les procédures pénales au sein de l'UE ont leur siège aux USA et qu'ils sont donc placés sous la souveraineté américaine, un accord entre l'UE et les USA doit permettre d'éviter d'éventuels conflits d'obligations entre les deux systèmes. L'objectif de l'UE est d'éviter, avec un accord international, des conflits de lois, notamment sur le plan des données relatives au contenu, et d'accélérer l'accès aux preuves électroniques. Étant donné que le droit américain en vigueur interdit aux CSPs américains de répondre aux requêtes d'autorités de poursuite pénale étrangères portant sur des données liées au contenu et que les autorités judiciaires et de poursuite pénale de l'UE rencontrent actuellement des difficultés pour collecter ces données au moyen de requêtes d'entraide pénale, un accord doit offrir un cadre juridique suffisant à ces autorités et permettre une collaboration directe avec les CSPs. Ainsi, du point de vue de l'UE, un accord entre l'UE et les USA permettrait avant tout de compléter l'objectif et l'efficacité des propositions sur les preuves électroniques, notamment en ce qui concerne les données liées au contenu détenues par un CSP américain basé aux USA.

³⁷ TSILIKIS, p. 169 ss et 172 ss

³⁸ Pour un aperçu complet, voir les explications dans la proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, consid. 47.

³⁹ Recommandation de la Commission européenne du 5 février 2019 pour une décision du Conseil autorisant l'ouverture de négociations en vue de la conclusion d'un accord entre l'Union européenne et les USA sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale, COM(2019) 70 final.

⁴⁰ Contenu disponible sur : <https://www.consilium.europa.eu/fr/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/>.

Rapport sur le US CLOUD Act (loi *Cloud*)

Concernant les données non liées au contenu, les autorités américaines invitent dès à présent les autorités de poursuite pénale et judiciaire de l'UE à s'adresser directement aux CSPs américains, si elles souhaitent collecter ces données compte tenu du nombre croissant de requêtes d'entraide pénale (voir l'introduction). À cet égard, le droit américain autorise les CSPs dont le siège est aux USA de donner suite à ces requêtes, sans toutefois les y contraindre. Un accord entre l'UE et les USA doit par conséquent améliorer la sécurité juridique également en ce qui concerne l'accès à des données non liées au contenu détenues par un CSP américain⁴¹.

Selon des contacts informelles, les négociations entre l'UE et les USA ne constituent pas des négociations « CLOUD-Act » à proprement parler. Leur objectif est plutôt d'établir une passerelle entre le *CLOUD Act* américain et la législation de l'UE sur les preuves électroniques. Tandis que, dans le cadre de ce processus, l'UE tente d'imposer son système de preuves électroniques, les USA souhaitent favoriser l'établissement du *CLOUD Act*. Deux approches exactement opposées ayant été choisies pour ces deux systèmes (USA : effet extraterritorial ; UE : obligation du CSP et/ou du représentant d'avoir une présence « territoriale »), ils ne sont donc pas pleinement compatibles. L'objectif est toutefois de pouvoir s'adresser directement aux CSPs des deux côtés de l'Atlantique, quel que soit le continent où leur siège est établi. En vertu de l'accord, les aspects juridiques relatifs à l'accès aux données liées ou non liées au contenu qui sont en possession des CSPs en Europe et aux USA, doivent être soumis aux mêmes prescriptions.

D'après des sources informelles, quatre séances de négociations ont eu lieu jusqu'à présent. La protection des données a occupé une place essentielle dans les discussions. Sur ce point, la Commission a déclaré que l'accord-cadre entre l'UE et les USA sur la protection des données devait être complété.⁴² D'importantes divergences subsistent encore sur de nombreux points. Cependant, il ne devrait pas être aisé pour la Commission d'avancer de manière substantielle dans les discussions, tant que les négociations en trilogue sur les preuves électroniques ne sont pas terminées. En effet, sa position dans les négociations dépend en grande partie de l'issue de cette procédure⁴³. La forme de l'accord reste à définir. Il devra en outre s'insérer dans le cadre juridique actuel⁴⁴, et les rapports entre ces différentes sources juridiques devront être clarifiés.

Les négociations avec les USA seront également influencées par les négociations menées parallèlement au sein du Conseil de l'Europe à propos d'un deuxième protocole additionnel à la Convention du Budapest. Ces dernières porteront sur des questions similaires et entraîneront des difficultés comparables car l'UE a une grande influence dans les négociations relatives à ce protocole (cf. point 4.3). Le contenu de ce protocole peut donc avoir des répercussions directes sur les négociations entre l'Union européenne et les USA⁴⁵.

⁴¹ Recommandation du 5 février 2019 pour une décision du Conseil autorisant l'ouverture de négociations en vue de la conclusion d'un accord entre l'Union européenne et les USA sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale, COM(2019) 70 final.

⁴² Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, JO L 336, 10.12.2016, p. 3–13).

⁴³ Report of the Commission services on the second round of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 6 novembre 2019, disponible sur : <https://www.statewatch.org/news/2019/nov/eu-council-usa-E-Evidence-13713-19.pdf>.

⁴⁴ Cf. p. ex. l'accord entre l'Union européenne et les USA en matière d'entraide judiciaire ainsi que la Convention de Budapest et les conventions bilatérales avec les États membres.

⁴⁵ Fiche d'information de la Commission européenne du 5 février 2019, questions et réponses : Mandat en vue du deuxième protocole additionnel à la convention de Budapest disponible sur : https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_19_865 (actualisé le 1.7.2020).

Rapport sur le US CLOUD Act (loi *Cloud*)

Une fois l'accord négocié, le Parlement européen doit encore approuver le texte de l'accord et le Conseil doit statuer sur la conclusion de l'accord.

4.3 Deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention du Budapest)⁴⁶

Le deuxième protocole additionnel à la Convention de Budapest qui est actuellement élaboré au sein du Conseil de l'Europe poursuit le même objectif de base que les instruments et procédures déjà mentionnés. Cet instrument doit lui aussi permettre aux autorités de poursuite pénale d'accéder plus facilement aux preuves électroniques. Il doit optimiser et accélérer la collaboration future entre les États contractants – parmi lesquels les USA – dans lesquels les principaux CSPs ont leur siège, lors des poursuites contre la *cyber-enabled criminality*. Cet instrument doit en particulier permettre aux autorités de poursuite pénale d'accéder plus facilement aux preuves électroniques, surtout quand ces dernières se trouvent à l'étranger. La collaboration avec les prestataires étrangers doit être facilitée.

Le protocole contient donc des dispositions qui doivent obliger les parties contractantes à créer dans leur législation nationale une réglementation permettant une collaboration directe avec les CSPs sur le territoire d'une autre partie contractante. Cela concerne l'accès à des informations sur les noms de domaine ou des données d'utilisateur, des méthodes garantissant une divulgation plus rapide des informations d'utilisateur, des données de connexion et, en cas d'urgence, des données enregistrées. D'autres dispositions précisent les conditions préalables à la collaboration ainsi que des clauses concernant les motifs d'irrecevabilité, en particulier la protection des données.

Les objectifs poursuivis dans le cadre du deuxième protocole additionnel, qui visent la suppression et la « délocalisation » de garanties fondées sur le droit et les procédures afin d'accélérer la coopération, sont cependant en contradiction avec l'exigence selon laquelle l'accord doit être ratifié dans le monde entier par le plus grand nombre possible d'États. Le Conseil de l'Europe a considérablement abaissé le seuil d'adhésion de pays tiers à la Convention de Budapest. Ainsi, des États qui parfois ne souhaitent pas ou ne sont pas en mesure de garantir les droits humains fondamentaux ni les garanties procédurales sont invités à adhérer à cette convention.

Concrètement, ce protocole peut aboutir à une collaboration simplifiée dans le cadre des poursuites pénales sans pour autant garantir un respect suffisant des garanties procédurales et des droits humains. Dans ce contexte, il est difficile d'imaginer la création d'une « *community of trust among the States Parties* » parfois citée, si le cercle des États contractants ne cesse de s'agrandir et si ces pays ne peuvent ou ne souhaitent pas respecter les garanties procédurales ni les droits fondamentaux, tels qu'ils sont perçus par la Suisse.

Les travaux du Conseil de l'Europe auraient dû être terminés en décembre 2020, mais cela n'a pas été possible en raison des divergences parfois importantes entre les délégations (points de vue divergents exprimés par la délégation américaine et divergences entre l'Australie, le Canada, le Japon d'une part et l'Union européenne d'autre part). Compte tenu du dilemme décrit ici entre d'une part l'universalisation du protocole et la simplification de la coopération et, d'autre part, les aspects en lien avec la protection juridique, on peut se demander si la Suisse cherchera à obtenir une signature rapide du protocole. À l'heure actuelle, une

⁴⁶ Convention sur la cybercriminalité du Conseil de l'Europe (Convention de Budapest), STE 185, RS 0.311.43 ; <https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185>.

Rapport sur le US CLOUD Act (loi *Cloud*)

procédure prudente, avec une analyse régulière des expériences et des répercussions à court et moyen terme, semble judicieuse.

Il convient d'ajouter que des travaux préparatoires en vue de la mise en place d'une convention mondiale sur la cybercriminalité ont débuté au niveau mondial sous l'égide de l'ONU. Il va de soi que les divergences mises en évidence par les discussions autour du deuxième protocole de la Convention de Budapest se manifestent ici avec une acuité encore plus forte. Ces travaux ne sont toutefois pas suffisamment avancés à l'heure actuelle ; c'est pourquoi, le présent rapport ne les aborde pas en détail.

5 Les questions juridiques

5.1 Territorialité et souveraineté

Le principe de territorialité est un pilier central du droit international, notamment en ce qui concerne les questions de délimitation dans le domaine de la compétence pénale. Il est étroitement lié à la souveraineté des États. En termes positifs, celle-ci comprend la compétence des États à s'organiser juridiquement et structurellement ainsi qu'à conclure des traités internationaux, et en termes négatifs, l'interdiction de s'immiscer dans les affaires intérieures d'autres États (interdiction d'intervention⁴⁷). L'interdiction pour les États de porter atteinte à la souveraineté et à l'intégrité territoriale d'autres États par leur législation ou leurs actions concrètes découle du principe de territorialité et des limites fixées par l'obligation de non-ingérence des États.

Dans l'*arrêt Lotus*⁴⁸ de 1927, qui reposait sur un incident en haute mer impliquant la France et la Turquie, la Cour Permanente de Justice Internationale (CPJI) a estimé que le principe de territorialité n'exclut pas des applications du droit au-delà de son propre territoire, tout du moins si celles-ci ne sont pas explicitement interdites par le droit international. Dans un arrêt de 1992, le Tribunal fédéral y fait également référence : « [L']application extraterritoriale de son propre droit [n'est] *a priori* pas non plus considérée comme inadmissible en droit international et en droit pénal international [...]. Au contraire, selon la doctrine et la pratique dominantes, la législation nationale peut également s'appliquer à des faits extraterritoriaux s'il existe une relation interne univoque entre ces faits et le droit national »⁴⁹.

Le commerce international, la mobilité mondiale et, en particulier, la communication moderne avec des données disponibles à l'échelle mondiale et accessibles à tout moment ne remettent pas fondamentalement en cause le principe de territorialité. Cependant, ils multiplient les points de contact et les risques de collision entre les différents ordres juridiques des États. Il est donc d'autant plus important de tracer des limites claires entre les applications de la loi hors du territoire de l'État, autorisées par le droit international, et les dépassements interdits de la compétence extraterritoriale. Les points de rattachement reconnus en droit international sont notamment le rattachement territorial (p. ex. la résidence ou le domicile d'une personne, le siège ou la succursale d'une société, le lieu d'exercice d'une activité) ou le rattachement personnel (p. ex. la nationalité de l'auteur ou de la victime d'un acte). Dans certains cas particuliers, pour préserver par exemple sa propre sécurité en cas d'attaques ou de menaces graves ou des intérêts fondamentaux généralement reconnus de la communauté internatio-

⁴⁷ Art. 2, al. 7 Charte des Nations Unies, RS 0.120.

⁴⁸ Publications de la Cour Permanente de Justice Internationale (CPJI), Recueil des Arrêts, Série A – n° 10, p. 18 ss, arrêt n° 9 : Affaire du « Lotus » du 7 septembre 1927.

⁴⁹ ATF 118 Ia 137 consid. 2b p. 142, traduit de l'allemand.

Rapport sur le US CLOUD Act (loi *Cloud*)

nale, comme la lutte contre les crimes les plus graves dans le cadre du principe d'universalité, un rattachement à un comportement matériel spécifique peut également être suffisant.

Le droit pénal reprend également ces principes de droit international⁵⁰. Cependant, en tant que dernier et plus radical moyen dont dispose un ordre démocratique pour défendre ses valeurs⁵¹, le lien avec la souveraineté et la territorialité est particulièrement étroit en droit pénal. Contrairement aux procédures civiles, les procédures pénales n'impliquent jamais la collaboration des parties – et surtout pas de la personne accusée. Au contraire, celle-ci peut revendiquer le principe selon lequel elle ne doit pas s'incriminer elle-même⁵². La collecte de preuves dans le droit de la procédure pénale inquisitoire des États d'Europe continentale est donc fondamentalement une tâche étatique. L'État établit, du moins selon la fiction, la vérité⁵³. La collecte des preuves en droit pénal est donc associée à des possibilités d'accès direct pour les autorités de poursuite pénale. En raison du rôle central des organes de l'État dans la collecte des preuves en droit pénal, l'État *sur le territoire duquel se trouvent les preuves* est fondamentalement responsable de sa réalisation. Le lieu d'un bien joue donc un rôle central dans la procédure pénale : l'autorité de poursuite pénale compétente sur le lieu de stockage est généralement responsable de la collecte des preuves matérielles. Jusqu'à présent, ce principe a également été transposé aux données qui doivent aussi être collectées sur le « lieu de stockage ».

Le *CLOUD Act* n'adhère à ces principes que dans une certaine mesure. Son champ d'application est très large en termes d'espace, de temps et de contenu (cf. point 3.2). Tous les CSPs basés aux USA sont couverts par la loi. Ainsi, la loi s'applique aux données stockées ou contrôlées par des CSPs étrangers en dehors des USA, si ces CSPs exploitent des succursales commerciales aux USA. Même des fournisseurs étrangers de services destinés au marché américain, qui résideraient à l'étranger, pourraient être concernés⁵⁴. D'une part, les autorités de poursuite pénale américaines peuvent sur la base du *CLOUD Act* collecter des données qui ne sont pas stockées aux USA. D'autre part, elles peuvent s'adresser à des entreprises qui ne sont pas basées aux USA et ne sont donc pas nécessairement soumises à leur juridiction. Ce deuxième cas de figure peut être considéré comme problématique au regard de la territorialité. Selon le *CLOUD Act*, les autorités américaines peuvent s'adresser directement à une personne privée (le CSP) sur le territoire de l'autre État, sans que celui-ci en soit informé. En outre, le CSP étranger ne dispose que de procédures américaines qui lui sont inconnues pour engager un recours, de sorte qu'il pourrait être désavantagé.

Même si cela ne remet pas fondamentalement en question le principe de territorialité en droit international, le champ d'application du *CLOUD Act* peut entraîner des *conflits de compétence extraterritoriale en droit pénal*. La question de la « tolérance » d'un tel accès extraterritorial aux données devrait être réglée dans un éventuel *executive agreement*.

5.2 Nature des *executive agreements*

Le *CLOUD Act* prévoit que les USA peuvent conclure des *executive agreements* avec d'autres États (cf. point 3.2.2). Sur la base de ces accords, les autorités de poursuite pénale de pays dotés d'un système constitutionnel démocratique (du point de vue des USA), de

⁵⁰ Voir à cet égard les principes de territorialité, de personnalité et du droit international sur lesquels la compétence pénale s'appuie.

⁵¹ Cf. FRANZ RIKLIN, *Schweizerisches Strafrecht, Allgemeiner Teil I, Verbrechenslehre*, Zurich 2007, §4 N 7.

⁵² Cf. art. 6, al. 1 CEDH et art. 113, al. 1, art. 140, art. 158, al. 1, let. b, art. 262, al. 2 et art. 265, al. 2, let. a CPP.

⁵³ Cf. art. 2 et art. 6 CPP.

⁵⁴ Voir le rapport à l'intention de l'Assemblée nationale française « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale » du 26 juin 2019, point 1.2.4.2.1, p. 29 ss ; disponible sur : https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2019/06/rapport_gauvain.pdf.

Rapport sur le US CLOUD Act (loi *Cloud*)

standards de protection des données et de garanties procédurales comparables à celles des USA doivent pouvoir contacter directement les CSPs aux USA, afin de collecter des données pour la poursuite de *serious crimes*. Dans le même temps, ces États partenaires tolèrent l'accès des autorités de poursuite pénale américaines aux données des CSPs situés sur leur territoire. Le cas échéant, les données sont communiquées directement entre le CSP et l'État « requérant » respectif, sans procédure d'entraide judiciaire.

Le *CLOUD Act per se* (c'est-à-dire même sans *executive agreement* additionnel) offre aux autorités de poursuite pénale américaines, comme cela a été expliqué, la possibilité d'obtenir l'accès à des données détenues et stockées par un CSP américain n'importe où dans le monde dans le cadre d'une procédure pénale engagée par l'administration américaine. Dans ce contexte, la possibilité de conclure des *executive agreements* avec d'autres États sous certaines conditions est un élément important pour promouvoir l'acceptation du *CLOUD Act*. Ce faisant, les USA s'appuient sur l'attractivité de leur pays dans le domaine de la fourniture de services de communication et offrent la réciprocité à leurs partenaires, afin de combler la lacune du *CLOUD Act* en matière de respect du principe de territorialité en droit international. Le manque de protection juridique est également abordé : si une procédure est ouverte aux USA contre un ressortissant étranger, les autorités américaines peuvent en principe demander la divulgation de ses données sur la base du *CLOUD Act*. Toutefois, il existe une exception concernant la divulgation des données d'un ressortissant étranger d'un pays avec lequel les USA ont conclu un *executive agreement*. Si un tel accord existe, les CSPs peuvent interposer une motion en modification ou en annulation en vertu du *CLOUD Act*, si leur client n'est pas une *US person* et si la divulgation des données risque de violer la loi du QFG. Un *executive agreement* pourrait donc offrir une certaine protection aux ressortissants suisses et aux personnes soumises à la juridiction suisse. Si la divulgation risque d'enfreindre la législation suisse, les CSPs pourraient engager une action en justice aux USA pour protéger les droits des personnes concernées. En conséquence, un *executive agreement* fournirait une certaine protection contre l'accès non autorisé des autorités de poursuite pénale américaines aux données (personnelles) en Suisse. La manière dont cette protection devrait être conçue afin de satisfaire aux exigences du droit suisse de rang supérieur est examinée ci-après aux points 5.5 et 5.6.

D'un point de vue formel, il convient de noter que le *CLOUD Act*, en tant que loi fédérale américaine, décrit lui-même les conditions préalables à la conclusion, le champ d'application matériel et les principaux contenus des *executive agreements*. Néanmoins, d'un point de vue formel, les *executive agreements* sont des traités bilatéraux qui relèvent de la Convention de Vienne sur le droit des traités⁵⁵. Ainsi, ce sont les règles générales du droit international et la pratique développée sur cette base qui s'appliquent à ces traités et à leur interprétation, et non, par exemple, le droit américain ou la jurisprudence américaine. L'application du droit américain ne serait possible que si un *executive agreement* faisait directement référence au droit américain. L'accord conclu entre les USA et le Royaume-Uni n'y fait pas référence⁵⁶. Il contient des obligations et des droits indépendants qui ne découlent pas du droit national. Du point de vue du droit international, les dispositions du *CLOUD Act* traitant des *executive agreements* s'apparentent donc plutôt à des « instructions » du législateur américain à l'adresse de son propre gouvernement.

En Suisse, les traités internationaux doivent être approuvés par l'Assemblée fédérale. Le Conseil fédéral les signe et les soumet à l'approbation de l'Assemblée fédérale. Après un

⁵⁵ Convention de Vienne sur le droit des traités du 23 mai 1969, RS 0.111.

⁵⁶ Agreement between the United Kingdom and the USA on Access to Electronic Data for the Purpose of Countering Serious Crime du 3 octobre 2019, note de bas de page 21.

Rapport sur le US CLOUD Act (loi *Cloud*)

vote favorable, il les ratifie (art. 184, al. 2 de la Constitution fédérale [Cst.]⁵⁷). Exceptionnellement, le Conseil fédéral peut conclure des traités de sa propre initiative. C'est le cas si sa compétence découle d'une loi ou d'un traité international (art. 166, al. 2 Cst.). Le cas échéant, l'Assemblée fédérale lui accorde par délégation le pouvoir de conclure des traités. En outre, le Conseil fédéral peut conclure seul des traités internationaux de portée mineure (art. 7a, al. 2 de la loi sur l'organisation du gouvernement et de l'administration [LOGA]⁵⁸).

Un *executive agreement*, tel que celui qui est réglé par le *CLOUD Act*, ne serait pas un traité de portée mineure. Comme il permettrait aux autorités suisses et américaines de collecter des données directement auprès des CSPs, il affecterait considérablement le droit de la protection des données et les garanties procédurales des personnes physiques ou morales concernées. En outre, bien que la législation suisse contienne une norme de délégation en faveur du Conseil fédéral dans le domaine de la protection des données (art. 67 nLDP), cette règle ne pourrait pas s'appliquer à un *executive agreement* basé sur le *CLOUD Act*. On peut donc supposer que l'approbation de l'Assemblée fédérale serait requise conformément à l'art. 184, al. 2 de la Constitution fédérale.

La conclusion d'un *executive agreement* aurait un impact considérable sur les cantons et les communes. D'une part, les données concernées sont celles qui relèvent de la législation cantonale sur la protection des données. D'autre part, il s'agit de procédures pénales qui relèvent principalement de la compétence des cantons. Même si la Confédération peut, sur la base de sa compétence en matière d'affaires étrangères (art. 54, al. 1 Cst.), conclure également des traités internationaux dans des domaines qui relèvent de la compétence des cantons, elle doit impérativement associer ces derniers si elle veut prendre des décisions de politique extérieure « affectant leurs compétences ou leurs intérêts essentiels » (art. 55, al. 1 Cst.). Dans ce cas, le Conseil fédéral doit informer les cantons en temps utile et de manière détaillée et il doit les consulter (art. 55, al. 2 Cst.). Ce serait vraisemblablement le cas pour la conclusion d'un *executive agreement*.

5.3 Notion de « *serious crime* » (infraction grave)

Les *executive agreements* peuvent servir de base à l'acquisition d'informations aux fins de prévention, de détection, d'enquête et de poursuite de *serious crimes*⁵⁹. Les infractions qui constituent des *serious crimes* au sens de l'*executive agreement* peuvent être par exemple clarifiées par le biais d'une liste d'infractions ou par la mention d'une peine minimale dans l'*executive agreement*.

La première variante (liste d'infractions) présente l'inconvénient d'être statique. La liste doit être constamment mise à jour et des contradictions pourraient apparaître en cas de modification de la loi.

La seconde variante (mention d'une peine minimale) est dynamique, mais contient un champ d'application potentiellement plus large (p. ex. tous les crimes et délits). Le fait que les infractions ne soient pas nécessairement qualifiées de la même manière dans les différents États se révèle être un défi. Si un acte est passible d'une peine élevée dans un État, il peut être puni de manière plus clémentaire ou ne pas l'être du tout dans un autre État. La question se pose donc de savoir si le critère des *serious crimes* doit être rempli dans les deux États, et donc si l'on applique une double incrimination « qualifiée » en conséquence, ou si l'accès aux

⁵⁷ RS 101

⁵⁸ RS 172.010

⁵⁹ DOJ, « Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act », p. 5.

Rapport sur le US CLOUD Act (loi *Cloud*)

données auprès d'un CSP est toléré même si l'acte n'est pas répréhensible dans son propre État.

Compte tenu de l'engagement toujours très fort des USA dans la lutte contre le terrorisme, il est prévisible qu'une couverture complète de la coopération dans le cas du « terrorisme » serait en tout cas un objectif américain pour un éventuel *executive agreement*. Cela n'est pas sans poser problème dans le contexte de la définition éventuellement plus étroite de l'organisation terroriste dans l'art. 260^{ter} CP⁶⁰ révisé. Des évaluations différentes particulièrement marquées et politiquement sensibles existeraient probablement dans le domaine de la *délinquance fiscale*. L'irrecevabilité générale de la *fraude fiscale* (cf. art. 3, al. 3 EIMP) n'est guère compatible avec les intérêts des USA. Il pourrait en être de même pour le domaine des *in-fractions contre l'honneur*. Aux USA, il existe une très grande liberté d'expression (*freedom of speech*), qui inclut en principe les discours de haine (*hate speech*), pour autant qu'ils ne soient pas considérés comme un appel direct à la violence. De nombreux discours de ce type auraient depuis longtemps été sanctionnés en Suisse, notamment au titre du délit de discrimination raciale (art. 261^{bis} CP).

Il semble donc qu'il serait difficile de trouver un standard commun pour le concept de « *serious crimes* » entre la Suisse et les USA.

5.4 Collecte de données électroniques

L'objectif du *CLOUD Act* et d'un *executive agreement* est de permettre la collecte transfrontière de données électroniques. Une question importante est donc de savoir quelles données peuvent être collectées auprès de qui et comment. De cette manière, il est possible d'évaluer si les modalités de collecte sont compatibles ou si elles doivent être adaptées.

Aux USA comme en Suisse, la législation vise les fournisseurs de services de télécommunication et les fournisseurs de services connexes.

5.4.1 Destinataires

La législation américaine établit une distinction entre les fournisseurs de services de communication électronique (*electronic communication services*) et ceux de services informatiques à distance (*remote computing services*). Un service de communication électronique correspond à toute offre de service qui permet à l'utilisateur d'envoyer ou de recevoir des communications filaires ou électroniques (*wire or electronic communications*)⁶¹. Les communications filaires sont des communications faisant appel à la voix humaine⁶². Les communications élec-

⁶⁰ Cf. FF 2020 7891.

⁶¹ « [A]ny service which provides to users thereof the ability to send or receive wire or electronic communications » (18 USC § 2510(15)).

⁶² « «[W]ire communication» means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce » (18 USC § 2510(1)). « «[A]ural transfer» means a transfer containing the human voice at any point between and including the point of origin and the point of reception » (18 USC § 2510(18)).

Rapport sur le US CLOUD Act (loi *Cloud*)

troniques s'effectuent via le transfert de données et à l'exclusion de toute communication faisant appel à la voix humaine⁶³. Les services informatiques à distance comprennent la fourniture publique de capacité de stockage ou de puissance de processeur par un service de communication électronique⁶⁴.

La Suisse fait une distinction entre les fournisseurs de services de télécommunication (« FST ») et les services de communication dérivés. Les services de télécommunication impliquent la « transmission d'informations pour le compte de tiers au moyen de techniques de télécommunication »⁶⁵, tandis que les services de communication dérivés « sont supportés par des services de télécommunication et permettent une communication unilatérale ou multilatérale »⁶⁶. Selon le message du Conseil fédéral, on entend par communication unilatérale le téléchargement ou le traitement en ligne de documents (p. ex. Google Docs ou Microsoft Office en ligne). Ainsi, les services de communication dérivés comprennent des offres d'hébergement web, des plateformes d'échange de documents et, enfin et surtout, des services de cloud⁶⁷. La communication multilatérale fait référence aux interactions entre les utilisateurs, au moyen de courriers électroniques, d'une messagerie instantanée ou d'une application VoIP comme Skype⁶⁸.

Dans ce contexte, la situation initiale dans les deux ordres juridiques (USA et Suisse) n'est certes pas « identique », mais elle n'est pas non plus différente au point qu'un accord sur une définition commune des destinataires dans un *executive agreement* serait impossible.

5.4.2 Type de données

Il existe également des points communs pour le type de données. De manière générale, on fait une distinction de part et d'autre de l'Atlantique entre les données personnelles, les données secondaires et les données de contenu. Les données personnelles (*basic subscriber information*⁶⁹), telles que définies dans la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT)⁷⁰, fournissent des informations sur le client et la relation contractuelle avec le fournisseur⁷¹. Les données secondaires au sens de la LSCPT ou les métadonnées (*transactional data*) indiquent avec qui, quand et comment la personne est

⁶³ « [E]lectronic communication» means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include — (A) any wire or oral communication ; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title) ; or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds » (18 USC § 2510(12)).

⁶⁴ « [T]he term «remote computing service» means the provision to the public of computer storage or processing services by means of an electronic communications system » (18 USC § 2711(2)).

⁶⁵ Art. 3, let. b Loi sur les télécommunications (LTC, RS **784.10**).

⁶⁶ Art. 2, let. c Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT, RS **780.1**).

⁶⁷ Explicitement dans le message, FF **2013** 2708.

⁶⁹ Celles-ci comprennent notamment le nom, l'adresse, le type et la durée du service utilisé, les instruments de paiement, y compris les numéros de carte de crédit et de compte : 18 USC § 2703(c)(2).

⁷⁰ RS **780.1**.

⁷¹ Cf. la définition de l'art. 18 al. 3 de la Convention de Budapest : « [T]oute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de services ;

b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;

c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services. »

Rapport sur le US CLOUD Act (loi *Cloud*)

en communication⁷². Enfin, le contenu (*content*) fait référence au message oral ou écrit proprement dit. Plus l'intervention de l'État se rapproche du cœur de la communication, c'est-à-dire du contenu, plus elle est intrusive et, par conséquent, plus elle doit être justifiée. Aux USA et en Suisse, les données personnelles peuvent être collectées sans autorisation judiciaire. La collecte de données secondaires et de contenu nécessite une autorisation judiciaire dans les deux pays. En Suisse, la collecte de données secondaires ou de contenu est une mesure de contrainte, mais la collecte de données personnelles ne l'est pas.

5.4.3 Modalités de collecte

Même si jusqu'à présent, la situation a paru similaire dans les deux pays, il existe cependant une différence importante au niveau des modalités de collecte des données. En Suisse, la collecte est effectuée par le service chargé de la surveillance de la correspondance par poste et télécommunication (service SCPT)⁷³. Celui-ci assure la fonction de plateforme entre les autorités et les CSPs : les ordres de surveillance et les données qui en découlent sont échangés via cette plateforme, si nécessaire avec l'autorisation du Tribunal des mesures de contrainte.

En revanche, le *CLOUD Act* part du principe que les CSPs sont directement sollicités et tenus de remettre les données. Cependant, cet accès direct aux CSPs poserait les problèmes suivants :

- Il serait contraire au système de permettre aux autorités américaines d'accéder directement aux CSPs alors que les autorités suisses doivent passer par le service SCPT. La question de l'égalité de traitement se pose. À cet égard, la question des coûts constitue un aspect important : les autorités suisses paient des frais élevés pour l'utilisation du service SCPT, qui ne seraient pas – ou pas de la même manière – encourus dans le cas d'un accès direct.
- Cela conduirait également à une collecte selon deux circuits : les CSPs, qui ont mis en place des procédures et des protocoles dans le cadre du SCPT pour les requêtes par le service SCPT, devraient servir parallèlement les autorités américaines par d'autres moyens.
- On peut se demander si la surveillance en temps réel serait possible de cette manière : la surveillance est généralement effectuée par le CSP sur ordre de l'autorité de poursuite pénale et sur décision du service SCPT, mais il suffit parfois qu'elle soit activée et tolérée par le fournisseur. Il semblerait que la surveillance nécessite des préparations techniques importantes, qui varient fortement d'un cas à l'autre. Par conséquent, on peut difficilement imaginer qu'elle puisse être réalisée dans le cadre d'une relation bilatérale entre une autorité américaine et un CSP suisse.
- Les décisions du service SCPT sont des décisions au sens de l'art. 5 de la loi fédérale du 20 décembre 1968 sur la procédure administrative (PA)⁷⁴. Le CSP concerné peut faire appel contre ces décisions (notamment contre celles ordonnant une surveillance pour exécuter un ordre de surveillance délivré/transmis par une autorité de poursuite

⁷² Voir la définition à l'art. 8, let. b LSCPT : « les données indiquant avec qui, quand, combien de temps et d'où la personne surveillée a été ou est en communication ainsi que les caractéristiques techniques de la communication considérée ».

⁷³ « Service chargé de la surveillance de la correspondance par poste et télécommunication, conformément à l'art. 269 du code de procédure pénale suisse (CPP) », cf. art. 3 LSCPT.

⁷⁵ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ; JO L 119/2016 du 4 mai 2016.

Rapport sur le US CLOUD Act (loi *Cloud*)

pénale) dans un cadre restreint. Cette possibilité pourrait *de facto* être encore plus limitée, voire suspendue, si le service SCPT ne joue plus aucun rôle ou ne transmet plus ces décisions.

Il serait concevable d'accorder également aux autorités américaines un accès via le service SCPT. Cependant, cela signifierait une extension massive des tâches pour le service SCPT. En outre, le texte du *CLOUD Act* n'est pas « adapté » à cette solution car il suppose que les données sont collectées directement auprès du CSP (toutefois, les ajustements nécessaires pourraient éventuellement être convenus dans l'*executive agreement*).

Les avantages d'une solution via le Service SCPT seraient évidents : en ce qui concerne la collecte des données, une égalité de traitement entre les autorités américaines et suisses serait établie (p. ex. les mêmes frais devraient être facturés aux autorités américaines). En outre, les autorités américaines auraient un point de contact unique (*single point of contact*), ce qui est dans tous les cas un avantage dans le trafic international des données. En poussant encore plus loin le raisonnement, le service SCPT pourrait ainsi jouer le rôle d'une autorité centrale pour la collecte des données américaines. Il serait alors possible de répondre aux craintes concernant la perte de la fonction de surveillance de l'OFJ : dans le cas de l'accès direct, tel que prévu par le *CLOUD Act*, il n'est pas précisé qui vérifie les motifs d'exclusion applicables à l'entraide judiciaire, qui contrôle le respect du principe de spécialité, etc. Toutefois, la manière dont la protection juridique du côté suisse pourrait fonctionner, comme décrit plus loin, reste également à définir (cf. point 5.6).

5.5 Protection des droits fondamentaux, en particulier protection des données et de la vie privée

5.5.1 Niveau européen : lien entre le *CLOUD Act* et le règlement général de l'UE sur la protection des données (RGPD)

5.5.1.1 Compatibilité du *CLOUD Act* et du RGPD

La compatibilité entre le *CLOUD Act* et un éventuel *executive agreement* conclu sur les principes de ce texte, d'une part, et de l'autre le droit européen, en l'occurrence le règlement général sur la protection des données⁷⁵ (RGPD), en vigueur depuis 2018, présente aussi une grande importance pour la Suisse. La Suisse n'étant pas membre de l'UE, le RGPD ne s'y applique pas directement puisqu'il ne s'agit pas d'un développement de l'acquis de Schengen. Mais ses dispositions s'appliquent aux entreprises en Suisse qui selon l'art. 3 RGPD relèvent du champ d'application du règlement. C'est le cas lorsque le CSP fournissant ses services est établi dans l'UE, ou s'il n'y est pas établi, lorsque les traitements de données sont liés à l'offre de biens ou de services à des personnes concernées dans l'Union ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

Afin de pouvoir échanger des données personnelles avec l'UE et ses pays membres, la Suisse doit continuer à être reconnue par la Commission européenne comme pays tiers assurant un niveau de protection adéquat, conformément à l'art. 45 RGPD. Pour que la *décision d'adéquation* soit maintenue, il est impératif que le droit suisse soit adéquat aux exigences du règlement en matière de protection des données. L'évaluation de la compatibilité du *CLOUD Act* et de l'éventuel *executive agreement* conclu sur la base de cette loi avec le RGPD a donc des conséquences sur la décision d'adéquation de l'UE dont la Suisse a besoin. Ceci est cor-

⁷⁵ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ; JO L 119/2016 du 4 mai 2016.

Rapport sur le US CLOUD Act (loi *Cloud*)

roboré par le fait que la Commission européenne, dans son évaluation du caractère adéquat de la protection des données assurée par le Royaume-Uni selon le RGPD, a examiné l'accord bilatéral conclu entre le Royaume-Uni et les USA sur la base du *CLOUD Act*, et plus particulièrement sa compatibilité avec la législation européenne relative à la protection des données⁷⁶. En revanche, dans le présent contexte, la situation au regard de la directive (UE) 2016/680⁷⁷ relative à la protection des données dans le cadre pénal n'est pas analysée. Certes, cette directive relève de Schengen, et à ce titre, elle doit être appliquée par la Suisse. Cependant, elle n'entre pas en considération dans la mesure où le *CLOUD Act* règle la transmission de données de CSPs privés *aux* autorités de poursuite pénale et non la transmission de données *par* les autorités (de poursuite pénale), qui sont les destinataires (exclusifs) de la directive. Enfin, l'accord RU-USA *CLOUD Act* ne semble pas avoir eu de pertinence pour l'évaluation par la Commission européenne de l'adéquation du niveau de protection des données du Royaume-Uni au regard de la directive (UE) 2016/680⁷⁸.

En résumé, il ressort de l'examen des bases juridiques déterminantes que les traitements de données réalisés sur injonction d'une autorité de poursuite pénale américaine dans le cadre du *CLOUD Act* peuvent être qualifiés de problématiques du point de vue de leur *légalité*. Ceci est vrai tout autant de la conservation de données personnelles que de leur divulgation.

Certes, tout comme le Comité Européen de la Protection des Données (EDPB) et le Contrôleur européen de la protection des données (CEPD), la Commission européenne reconnaît elle aussi que sur la base de l'art. 6 et plus particulièrement de l'art. 49 RGPD, dans des situations exceptionnelles déterminées, un traitement de données, voire la transmission de données à un État tiers, peut être justifié même quand cet État ne dispose pas d'une décision d'adéquation de la Commission européenne ni de garanties appropriées relatives à la protection des données (art. 46 RGPD). Ce serait notamment le cas si la divulgation des données personnelles par le CSP était nécessaire à la *sauvegarde des intérêts vitaux de la personne concernée* (art. 6, al. 1, let. d en rapport avec art. 49, al. 1, let. f RGPD). Par ailleurs, il n'est pas exclu qu'un tel transfert de données puisse être justifié par des motifs importants d'intérêt public (art. 49, al. 1, let. d RGPD) reconnus dans l'UE et ses pays membres, par exemple dans l'hypothèse où il existerait des indications concrètes concernant une infraction pénale grave ou un attentat terroriste en préparation dans l'UE. Cependant, dans la pratique, on peut supposer que cette situation dérogatoire ne serait que très rarement constituée, le RGPD ne permettant de tels transferts liés à des risques particuliers pour les droits et les libertés des personnes concernées qu'à des conditions très strictes et dans des situations absolument exceptionnelles.

⁷⁶ Décision d'exécution de la Commission du 28 juin 2021 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni ; C(2021) 4800 final, chiffres 153-156.

⁷⁷ Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ; JO L119/89 du 4.5.2016.

⁷⁸ Décision d'exécution de la Commission du 28 juin 2021 constatant, conformément à la directive (UE) 2016/680 du Parlement européen et du Conseil, le caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni ; C(2021) 4801 final. Afin de prendre en compte l'avis 15/2021 du Comité Européen de la Protection des Données sur la décision d'adéquation du Royaume-Uni selon la directive (UE) 2016/680, qui porte un regard extrêmement critique sur les injonctions de surveillance par écoute, notamment celles figurant dans l'accord bilatéral conclu par le Royaume-Uni et les USA sur le *CLOUD Act*, la Commission européenne a complété sa décision. Dans le cadre de la surveillance des futures évolutions concernant la protection des données au Royaume-Uni, elle accordera une attention particulière à la conclusion d'accords internationaux ayant des effets sur le niveau actuel de protection des données (point 165 de cette décision). Cependant, même si la directive (UE) 2016/680 est interprétée dans l'UE comme portant non seulement sur les transmissions de données, mais aussi sur les traitements de données effectués par des autorités de poursuite pénale, le champ d'application de cette directive est interprété de manière plus étroite en Suisse, et ne nous semble pas remis en cause présentement.

Rapport sur le US CLOUD Act (loi *Cloud*)

De même, le traitement des données sur la base du *CLOUD Act* pourrait s'avérer problématique en ce qui concerne d'autres éléments clés du RGPD :

Du point de vue de la transparence, le fait que les autorités américaines de poursuite pénale ne soient pas obligées, dans certains cas, d'informer les personnes concernées de la communication des données, et qu'elles puissent même, par voie de décision judiciaire, obliger le CSP à ne pas en informer la personne concernée, pourrait être problématique⁷⁹. Dans la conception européenne du droit, même en matière de poursuite pénale et d'exécution des peines, on considère qu'il est impératif que la personne concernée soit informée de l'accès des autorités à ses données personnelles⁸⁰. Selon la Cour de justice de l'UE (CJUE), la personne concernée doit être informée de la communication de ses données personnelles à des autorités étrangères de poursuite pénale, au plus tard lorsque cela ne risque plus de nuire aux investigations correspondantes⁸¹.

Du point de vue de la proportionnalité, le EDPB et le CEPD parviennent à la conclusion que dans l'ensemble, le *CLOUD Act* respecte ce principe⁸². Ainsi, une autorité américaine de poursuite pénale ne peut exiger la divulgation de données personnelles que si un tribunal l'a au préalable autorisée et si l'autorité expose, dans une déclaration sur l'honneur, qu'elle dispose de suffisamment d'éléments pour soupçonner qu'un crime défini a été commis ou est en train d'être commis et que les informations réclamées contiennent la preuve de ce crime précis⁸³. L'injonction de production doit en outre contenir une description exacte des données personnelles demandées, les recherches à l'aveuglette ou *fishing expeditions* destinées à trouver des preuves n'étant pas admises⁸⁴. Mais les autorités européennes de protection des données constatent aussi que dans le cas d'autres formes de requêtes, aucun contrôle judiciaire correspondant n'est exigé⁸⁵. Il faudrait ici décider au cas par cas si un traitement de données est proportionnel ou pas.

Contrairement au RGPD, qui accorde la même protection aux données personnelles de toutes les personnes physiques, quelle que soit leur nationalité ou leur lieu de résidence, le *CLOUD Act* fait une distinction entre les données des *US persons* et celles des autres personnes. En particulier dans le cas où il existe un *executive agreement*, un CSP ne peut exiger le contrôle judiciaire d'une injonction émanant d'une autorité américaine de poursuite pénale en cas d'obligations juridiques contradictoires, que s'il ne s'agit pas de données personnelles de *US persons*⁸⁶. En revanche, selon le CEPD, toute inégalité de traitement fondée sur la nationalité ou le lieu de résidence de la personne concernée est incompatible avec le RGPD⁸⁷.

Le *CLOUD Act* ne prévoit pas de garanties en matière de protection des données pour les personnes concernées, par exemple sous la forme d'un droit d'accès ou d'un droit de consultation de leurs données. Au contraire, il permet de renoncer entièrement, dans certains cas, à informer les personnes concernées que des données les concernant ont été transmises à

⁷⁹ *CLOUD Act*, § 2703 (b) (1) et § 2705 (b).

⁸⁰ Cf. entre autres CJUE, Avis 1/15 Accord PNR UE-Canada, ECLI:EU:C:2017:592, point 220 et avis 23/2018 du CEPD, p. 19.

⁸¹ CJUE, Avis 1/15 Accord PNR UE-Canada, ECLI:EU:C:2017:592, point 220.

⁸² EDPB/CEPD, Initial legal assessment, p. 2.

⁸³ DOJ, « Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the *CLOUD Act* », p. 8.

⁸⁴ Idem, p. 8.

⁸⁵ EDPB/CEPD, Initial legal assessment, p. 2.

⁸⁶ *CLOUD Act*, § 2703.

⁸⁷ Avis 2/2019 du CEPD, chiffre 50.

Rapport sur le US CLOUD Act (loi *Cloud*)

une autorité américaine de poursuite pénale⁸⁸. Cela va à l'encontre de l'art. 8, al. 2 de la Charte européenne des droits fondamentaux⁸⁹, qui garantit explicitement le droit pour toute personne d'accéder aux données personnelles collectées la concernant et d'en obtenir la rectification.

Le *CLOUD Act* ne prévoit aucune possibilité, pour la personne concernée par une injonction de production, de se défendre face à la divulgation de ses données personnelles. Dans les cas de conflits de droit, une possibilité restreinte de défense est uniquement prévue pour le CSP, et seulement à la condition qu'un *executive agreement* ait été conclu entre les USA et l'État correspondant⁹⁰. En revanche, la personne concernée par une injonction de ce type ne peut ni saisir une autorité de contrôle indépendante, ni exercer un recours judiciaire pour s'opposer à la transmission. L'absence de droit à un recours effectif devant un tribunal est contraire à l'art. 47 de la Charte européenne des droits fondamentaux, qui garantit le droit à une protection juridique et judiciaire efficiente. La CJUE insiste par ailleurs sur l'importance, pour toute personne concernée, de pouvoir déposer un recours administratif auprès d'une autorité nationale de contrôle⁹¹.

L'art. 8, al. 3 de la Charte européenne des droits fondamentaux prévoit, comme garantie essentielle de la protection des données, un contrôle exercé par une autorité indépendante. À cet égard, le CEPD insiste sur le fait que les autorités compétentes de l'État sur le territoire duquel se trouvent les données personnelles demandées doivent être impliquées dans les processus de transmission de preuves électroniques, afin de garantir efficacement la protection des droits fondamentaux⁹². De la même manière, les autorités compétentes en matière de protection des données devraient elles aussi être informées, en cas d'injonctions directement adressées aux prestataires, de manière à pouvoir exercer un contrôle⁹³. Dans ce contexte, le fait que les CSPs transmettent des données personnelles à une autorité américaine de poursuite pénale sans en informer les autorités compétentes de leur propre pays pourrait se révéler problématique.

5.5.1.2 Bilan : risques liés à la conclusion d'un *executive agreement* avec les USA pour la décision d'adéquation de la Suisse

La *décision d'adéquation* évoquée au chiffre 5.5.1.1 est évaluée régulièrement par la Commission, à savoir au moins tous les quatre ans (art. 97 RGPD). Les principaux aspects pris en compte lors de cet examen sont les règles de protection des données, les règles concernant la transmission de données personnelles vers un pays tiers et la conclusion d'accords internationaux relatifs à la protection des données personnelles. Dans l'arrêt *Schrems II*, la CJUE a précisé, en ce qui concerne l'accès des autorités aux données personnelles transmises dans l'État destinataire à des fins de sécurité nationale, que la Commission, pour prendre sa décision, doit tenir compte du droit national applicable dans l'État destinataire. Le critère décisif de l'adéquation est de savoir si la réglementation qui autorise l'ingérence des autorités dans l'État destinataire à des fins de sécurité nationale contient également des dispositions claires sur la limitation de cette ingérence, et donc précise clairement à quelles conditions et dans quelles circonstances elle peut être permise. L'accès aux données doit s'opérer

⁸⁸ *CLOUD Act* § 2703 (b) (1) et § 2705 (b).

⁸⁹ Charte européenne des droits fondamentaux, JO 2000/C 364/01 du 18.12.2000.

⁹⁰ Cf. plus haut, chiffre 3.2.2.

⁹¹ Arrêt de la CJUE, *Maximilian Schrems contre Data Protection Commissioner*, C-362-14, ch. marg. 56 – 58.

⁹² Avis 2/2019 du CEPD, chiffre 28. Dans le contexte des injonctions européennes de production et de conservation de preuves électroniques en matière pénale, voir aussi l'avis 23/2018 du EDPB, p. 16.

⁹³ Voir l'avis 23/2018 du EDPB, p. 8.

Rapport sur le US CLOUD Act (loi *Cloud*)

dans les limites du strict nécessaire⁹⁴. D'autre part, la réglementation correspondante doit prévoir dans l'État destinataire des droits effectifs et opposables afin de protéger les personnes concernées contre d'éventuels abus⁹⁵.

En 2000, la Suisse a reçu de l'UE la confirmation qu'elle offrait un niveau de protection des données adéquat. Pour l'instant, cette décision d'adéquation continue d'être valable sous l'angle du RGPD, applicable depuis le 25 mai 2018. Au printemps 2019, la Commission européenne a commencé une nouvelle évaluation de la Suisse. Elle réalise cet examen sur la base du droit suisse en vigueur, mais s'est déclarée prête à prendre en compte le renforcement de la protection des données qu'entraînera la révision de la loi fédérale sur la protection des données (LPD), à condition que la révision totale de cette dernière soit achevée en temps utile. La nouvelle loi fédérale sur la protection des données (nLPD) ayant été adoptée par les Chambres fédérales le 25 septembre 2020 (voir plus bas, 5.5.2.1), et son entrée en vigueur, comme celle des ordonnances correspondantes, étant prévues pour le second semestre 2022, cette condition devrait être remplie.

Dans sa décision concernant le caractère adéquat du niveau de protection des données personnelles assuré par le Royaume-Uni conformément au RGPD, qui a été adoptée le 28 juin 2021 par la Commission européenne en même temps que la décision sur l'adéquation du Royaume-Uni selon la directive (UE) 2016/680, la Commission a évalué également l'accord bilatéral conclu par le Royaume-Uni et les USA sur la base du *CLOUD Act*⁹⁶. Cela montre que le contenu d'un *executive agreement* conclu entre la Suisse et les USA serait lui aussi pris en compte dans la perspective d'une nouvelle évaluation du caractère adéquat du niveau de protection des données garanti par la Suisse.

Dans la décision relative au Royaume-Uni, la Commission européenne note que lors de l'entrée en vigueur de l'accord bilatéral conclu par le Royaume-Uni et les USA sur la base du *CLOUD Act*, les données transférées depuis l'UE vers des CSPs au Royaume-Uni pourraient faire l'objet d'injonctions de production émanant des autorités de poursuite pénale des USA. Une évaluation des conditions et des garanties auxquelles de telles injonctions peuvent être exécutées est donc pertinente dans la perspective de la décision d'adéquation du niveau de protection des données garanti par le Royaume-Uni. Certes, la Commission n'estime pas que l'accord, au regard des exigences du RGPD, soit inadéquat en tant que tel. D'une part, la Commission européenne souligne qu'elle est elle-même mandatée par les pays membres pour mener des négociations avec les USA dans ce domaine, et que de ce fait, il ne faudrait pas créer de « *double standard* » quant à un accord correspondant entre le Royaume-Uni et les USA. D'autre part, la Commission juge positives les exigences strictes fixées dans l'accord en matière d'injonctions de production et de surveillance en temps réel, de même que le fait que par un renvoi à l'accord-cadre conclu entre l'UE et les USA⁹⁷, toutes les garanties et les droits définis dans ce dernier soient applicables par analogie⁹⁸. La Commission retient en outre que les autorités britanniques lui ont confirmé que l'accord n'entrerait en vigueur que lorsque le respect de ces standards en matière de protection des données serait garanti pour toutes les données transférées dans le cadre de cet accord.

⁹⁴ CJUE, *Schrems II*, consid. 175-176.

⁹⁵ CJUE, *Schrems II*, consid. 177-178.

⁹⁶)» (. Chiffres 153 - 156 de la décision sur l'adéquation relative au Royaume-Uni selon le RGPD.

⁹⁷ Voir la note de bas de page 41

⁹⁸ L'art. 9, al. 1 de l'accord bilatéral conclu par le Royaume-Uni et les USA sur la base du *CLOUD Act* note qu'une protection équivalente à celle prévue par cet accord-cadre « s'applique à toutes les données personnelles collectées lors de l'exécution d'injonctions produites sur la base de l'accord. »

Rapport sur le US CLOUD Act (loi *Cloud*)

Le EDPB⁹⁹ et le Parlement européen¹⁰⁰ se montrent nettement plus sceptiques. Ils doutent, notamment, qu'une simple référence à l'accord-cadre UE-USA suffise pour que les droits en matière de protection des données qui y sont garantis puissent être effectifs et opposables selon le droit britannique et que les mesures de protection qui y sont prévues s'appliquent à toutes les injonctions de production des autorités américaines de poursuite pénale – et se demandent donc si le droit américain ne prévaudrait pas tout de même. Face à ces craintes, la Commission affirme que la décision d'adéquation prévoit une surveillance permanente des évolutions relatives à ces questions. Elle précise qu'elle accordera une attention particulière à l'application et à la mise en œuvre des garanties contenues dans l'accord-cadre lors des transferts de données correspondants, et tirera les conséquences qui s'imposent si certains signes indiquent qu'un niveau de protection adéquat n'est plus garanti. Une mesure essentielle préconisée à cet égard par la Commission européenne est la « *sunset clause* », qui figure à l'art. 4 de la décision d'adéquation, et selon laquelle la décision d'adéquation du niveau de protection garanti par le Royaume-Uni expirera automatiquement au bout de quatre ans, si aucun accord supplémentaire n'est adopté.

Même si, selon la Commission européenne, l'accord entre le Royaume-Uni et les USA garantit les standards de protection des données applicable dans l'UE, la situation de départ est différente pour la Suisse. De fait, le Royaume-Uni, à l'exception du domaine du contrôle de l'immigration¹⁰¹, applique encore l'intégralité du RGPD, du moins pour l'instant – ce qui n'est pas le cas de la Suisse. De plus, la référence à l'accord-cadre conclu entre l'UE et les USA et l'affirmation correspondante des autorités britanniques de ne laisser entrer en vigueur l'accord que si les garanties correspondantes sont assurées, permettent à la Commission de considérer que les données personnelles transmises sur la base de l'accord bilatéral conclu par le Royaume-Uni et les USA sur la base du *CLOUD Act* continuent à bénéficier de la protection d'un instrument juridique de l'UE.

À cet égard, les possibilités pour la Suisse semblent plus limitées. Du fait du cadre étroit et problématique du point de vue de la protection des données du *CLOUD Act*, on ne peut supposer que la Suisse, par la conclusion d'un *executive agreement*, pourrait satisfaire aux exigences décrites plus haut dans le domaine de la protection des données. C'est pourquoi, la Commission, en menant ses propres négociations avec les USA, poursuit l'objectif d'un accord global qui réglerait les échanges de preuves électroniques et irait donc plus loin qu'un *executive agreement* tel que le *CLOUD Act* le prévoit. La Suisse ne pourrait donc sans doute obtenir la protection juridique complète, qui est exigée par la législation européenne en matière de protection des données et qui est garantie dans le cas du Royaume-Uni selon l'avis de la Commission, que par la conclusion d'un accord *global* avec les USA. Cet accord devrait réglementer les échanges de preuves électroniques et prévoir simultanément un haut niveau de protection des données correspondant aux standards européens et nationaux. Enfin, pour satisfaire également aux exigences de l'EDPB, il faudrait garantir qu'un tel accord *prévale sur le droit américain* en cas d'échange de données entre un CSP et des autorités de poursuite pénale.

⁹⁹ Avis 14/2021 du 13 avril 2021 du EDPB sur le projet de décision d'exécution de la Commission européenne constatant, conformément au règlement (UE) 2016/679, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni, ch. marg. 88 ss

¹⁰⁰ Résolution du Parlement européen du 21 mai 2021 sur le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni (2021/2594 (RSP)), ch. 25.

¹⁰¹ Compte tenu de l'arrêt de la *Court of Appeal* du Royaume-Uni du 26 mai 2021, par lequel les réglementations d'exception des prétentions relatives à la protection des données prévues au Royaume-Uni dans le domaine du contrôle de l'immigration sont jugées incompatibles avec le RGPD, la Commission européenne exclut dans un premier temps ce domaine de la décision d'adéquation prévue conformément au RGPD. Dès qu'il sera établi que le Royaume-Uni corrigera ces défauts, et de quelle manière, la Commission étudiera la possibilité d'une réintégration de ce domaine et modifiera éventuellement la décision en conséquence (chiffre 6 de la décision sur l'adéquation relative au Royaume-Uni selon le RGPD).

Rapport sur le US CLOUD Act (loi *Cloud*)

En outre, on peut supposer que la Commission européenne accordera, pour les futures décisions d'adéquation, plus de poids aux réserves formulées par l'EDPB et le Parlement européen au sujet de l'accord bilatéral conclu entre le Royaume-Uni et les USA sur la base du *CLOUD Act* que dans le cas du Royaume-Uni. Ici, l'urgence de trouver une base juridique aux transferts de données depuis l'UE vers le Royaume-Uni à l'issue de la période de transition semble avoir été un facteur déterminant qui a poussé la Commission à ne pas dévier de son projet, malgré la résistance du Parlement et de l'EDPB, d'adopter les décisions d'adéquation relatives au Royaume-Uni avant la fin du mois de juin 2021. Comme déjà mentionné, ces décisions ont été adoptées le 28 juin 2021 et sont de durée limitée, valides jusqu'en 2025.

Dans ses décisions d'adéquation relatives au Royaume-Uni, la Commission européenne insiste sur le fait qu'elle appuie pour l'essentiel ses évaluations sur l'arrêt *Schrems II* de la CJUE (arrêt du 16 juillet 2020). Cela devrait inciter la Suisse à adopter une démarche prudente, étant donné que la Cour de justice y indique que la Commission européenne, dans sa décision sur le caractère adéquat de la communication de données aux USA dans le cadre du *Privacy-Shield*, n'a pas tenu compte du fait que les dispositions relatives aux programmes de surveillance nationaux n'offrent, selon le droit américain, pas de garanties suffisantes de respect des exigences du RGPD en matière de protection des données, et pas non plus de protection juridique suffisante aux personnes concernées n'entrant pas dans la catégorie des *US persons*¹⁰². On peut en déduire que la Commission européenne sera encore plus stricte, lors de ses futures décisions d'adéquation, dans l'évaluation des garanties offertes par les accords internationaux pour combler de telles lacunes en matière de protection des données. En outre, les alignements d'autres actes juridiques sur la directive (UE) 2016/680¹⁰³, entrepris actuellement dans le domaine des poursuites pénales et de l'exécution des peines, montrent qu'à l'avenir, l'UE sera encore plus stricte dans son application des conditions d'échanges de données dans ces domaines.

5.5.2 Licéité du traitement des données et des divulgations fondées sur une injonction de production basée sur le *CLOUD Act* sous l'angle du droit suisse

5.5.2.1 Aspects pertinents du cadre juridique de la protection des données en Suisse

Au niveau fédéral, la protection des données est actuellement régie prioritairement par la loi fédérale du 19 juin 1992 sur la protection des données (LPD)¹⁰⁴. L'objet de la LPD est le traitement des données par les organes fédéraux comme par les personnes physiques. En outre, de nombreux standards de protection des données spécifiques à des domaines particuliers contenus dans des lois spéciales règlent les traitements de données effectués par les organes de la Confédération. Pour le traitement de données par les organes fédéraux et les particuliers, d'autres textes s'appliquent également, à savoir l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD)¹⁰⁵ et l'ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données (OCPD)¹⁰⁶. Le traitement de données par des organes cantonaux ou communaux est réglé dans les lois cantonales relatives à la protection des données.

¹⁰² CJUE, *Schrems II*, consid. 175-178.

¹⁰³ Cf. « Communication from the Commission to the European Parliament and the Council : Way forward on aligning the former third pillar acquis with data protection rules », disponible sur https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v7.pdf (version 7.6.2021).

¹⁰⁵ RS 235.11

¹⁰⁶ RS 235.11

¹⁰⁶ RS 235.13

Rapport sur le US CLOUD Act (loi *Cloud*)

Le 25 septembre 2000, le Parlement a adopté la révision totale de la LPD (nLPD)¹⁰⁷. La consultation sur l'OLPD révisée est en cours. En l'état actuel des choses, l'entrée en vigueur de la législation révisée relative à la protection des données est prévue pour le second semestre 2022. Avec cette révision totale, la législation suisse sur la protection des données sera considérablement renforcée et rapprochée du niveau de protection européen.

Dans la question de la compatibilité du traitement des données effectué sur la base d'injonctions de production avec la législation suisse en matière de protection des données, les textes déterminants sont la LPD en vigueur, l'OLPD ainsi que les dispositions pertinentes de la LPD totalement révisée (OLPD incluse). En revanche, dans le présent contexte, il n'est pas nécessaire de prendre spécialement en compte la loi fédérale du 28 septembre 2018 sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (LPDS)¹⁰⁸, compte tenu de son champ d'application, ni la Convention révisée 108+ du Conseil de l'Europe, ratifiée par la Suisse. Par son contenu, cette dernière est très proche de la directive (UE) 2016/680 et du RGPD ; les principes qui y sont énoncés ont été pris en compte dans le cadre de la révision de la LPD.

5.5.2.2 Aspects problématiques au regard des principes de la protection des données en Suisse

La législation suisse sur la protection des données repose sur un autre présupposé que le RGPD, selon lequel le traitement de données par des personnes physiques est fondamentalement illicite à moins qu'il ne soit dûment justifié par un motif valable. En Suisse, les traitements de données effectués par des personnes privées sont autorisés pour autant qu'ils ne portent pas atteinte à la personnalité. Il y a notamment atteinte à la personnalité quand un traitement de données enfreint les principes généraux de l'art. 4 LPD/art. 6 nLPD (en particulier la licéité, la bonne foi, la proportionnalité, le traitement limité au but indiqué et les finalités reconnaissables pour la personne concernée) ou que les exigences en matière d'exactitude des données (art. 5 LPD/art. 6, al. 5 nLPD) et de sécurité des données (art. 7 LPD/art. 8 nLPD) ne sont pas remplies (art. 12, al. 2, let. a LPD, art. 30, al. 2, let. a nLPD)¹⁰⁹. En général, ces principes sont repris tels quels dans la législation révisée. En sus de ces principes de protection des données, les divulgations de données à l'étranger doivent respecter les exigences de l'art. 6 LPD¹¹⁰, qui ont été reprises aussi dans le droit révisé (art. 16 s. nLPD).

Au regard des principes de protection des données, les traitements de données effectués sur la base du *CLOUD Act* semblent problématiques à différents égards. Ainsi, le principe de la bonne foi exige que les règles générales liées au traitement des données s'appliquent. Ceci reste valable lorsque les prescriptions et garanties se rapportant à la protection des données sont incomplètes ou ne sont pas concrètes. Ceci concerne notamment la question de la transparence du traitement des données. Dans ce contexte, les traitements de données effectués suite à des injonctions de production pourraient être problématiques à plusieurs égards. La divulgation de données en dehors du cadre d'une requête d'entraide judiciaire peut être considérée comme une infraction au principe de la bonne foi. Et on peut en dire autant des traitements de données qui se font à l'insu de la personne concernée¹¹¹. Une autre

¹⁰⁷ FF 2020 7397

¹⁰⁸ RS 235.3

¹⁰⁹ BRUNO BAERISWYL dans : BAERISWYL BRUNO (Éditeur), Stämpflis Handkommentar zum Datenschutzgesetz (SHK DSG), Berne 2015, remarques préliminaires concernant l'art. 4 – 11a, ch. marg. 3.

¹¹⁰ MAURER-LAMBROU/STEINER dans BSK DSG et BGÖ, art. 6 LPD, ch. marg. 11a.

¹¹¹ Message LPD, FF 1988 II 421 (457).

Rapport sur le US CLOUD Act (loi *Cloud*)

disposition du *CLOUD Act* pourrait se révéler problématique, à savoir celle qui interdit totalement d'informer la personne concernée avant que les autorités n'accèdent aux données.

Il découle du principe de proportionnalité que seules les données aptes et nécessaires à atteindre les finalités du traitement peuvent être traitées. Il doit y avoir un rapport raisonnable entre les finalités et le moyen utilisé, et les droits de la personne concernée doivent être préservés dans la plus large mesure possible¹¹². Ce principe s'applique aussi aux personnes physiques qui traitent des données. Il convient en cela de toujours concilier les intérêts des personnes concernées et ceux du responsable du traitement. Dans la mesure où le *CLOUD Act* prévoit une vérification judiciaire dans le cadre des injonctions de production (voir le point 3.2.1), on peut partir du principe que le principe de proportionnalité est bien respecté. En revanche, le fait que, pour d'autres formes de requêtes, aucun contrôle de ce type ne soit prévu pourrait se révéler problématique du point de vue de la proportionnalité. Par ailleurs, pour ce qui est de la nécessité, il convient d'examiner si la voie de la requête d'entraide judiciaire classique n'aboutirait pas au même résultat, et s'il ne faudrait pas la privilégier dans la mesure où elle constituerait une mesure plus « douce », entraînant une atteinte moins radicale aux droits de la personnalité de la personne concernée.

Les données doivent toujours être collectées pour des finalités déterminées et reconnaissables pour la personne concernée. Lorsque des personnes physiques traitent des données personnelles, la finalité de ce traitement est principalement déterminée par les informations fournies à la personne concernée lors de la collecte de ses données ou qui ressortent des circonstances. La personne concernée doit pouvoir comprendre ce qu'il advient de ses données. Un traitement ultérieur des données personnelles pour une finalité différente, que les personnes concernées peuvent légitimement considérer comme inattendu ou non reconnaissable, violerait leur droit à la vie privée et à l'autodétermination en matière d'information, à moins que ce changement de finalité ne soit justifié, par exemple, par leur consentement. Si des données personnelles sont conservées ou communiquées à des autorités américaines de poursuite pénale sur la base d'injonctions de production telles que celles prévues par le *CLOUD Act*, cela représente une modification de la finalité initialement prévue par les CSPs dans le cadre de leurs prestations contractuelles. Dans pareil cas, la loi exige que cette modification de finalité soit dûment justifiée par un motif et que les personnes concernées en soient informées.

Le principe de reconnaissabilité exige que la collecte des données, comme les finalités du traitement, soient reconnaissables pour la personne concernée. Ce principe est la condition du droit à l'autodétermination en matière d'information et de l'exercice des droits liés à la protection des données. Il découle de ce principe que les responsables du traitement sont tenus d'informer les personnes concernées, à moins que le traitement de leurs données ne soit pour elles clairement reconnaissable¹¹³. Sous cet angle aussi, les traitements de données effectués sur la base d'injonctions de production émanant des autorités des USA paraissent problématiques puisqu'elles s'appuient sur un droit étranger. De plus, il faudrait aussi examiner si le fait qu'une autorité américaine de poursuite pénale puisse interdire à un CSP, par voie de décision judiciaire, d'informer la personne concernée de la transmission de ses données pourrait être compatible avec le principe de transparence ou éventuellement justifié. L'information doit cependant être donnée au plus tard dès que cela ne risque plus de nuire à d'éventuelles investigations.

¹¹² Message LPD, FF 1988 II 421 (458).

¹¹³ BAERISWYL, SHK DSG, art. 4, ch. marg. 47-50.

Rapport sur le US CLOUD Act (loi *Cloud*)

5.5.2.3 Motifs justificatifs pour les personnes physiques en cas d'atteinte à la personnalité, art. 13 LPD/art. 27 nLPD

Les motifs possibles justifiant qu'un traitement de données ne soit pas considéré comme une atteinte à la personnalité illicite sont : le consentement de la personne concernée, un intérêt prépondérant privé ou public, ou un traitement justifié par la loi. Cependant, selon la jurisprudence du Tribunal fédéral, une infraction aux principes de protection des données de l'art. 4, de l'art. 5, al. 1 et de l'art. 7, al. 1 LPD (ou art. 6 et 8 nLPD) ne peut être justifiée que dans de très rares cas¹¹⁴.

Une atteinte à la personnalité peut être justifiée par le fait que la personne concernée consent au traitement des données. Pour que ce consentement soit juridiquement valable, il faut que la personne concernée ait été correctement informée de ce traitement de données. Ces informations doivent lui permettre d'évaluer les risques qui existent pour ses droits de la personnalité. Pour être correcte, l'information doit donc aussi mentionner les risques spécifiques d'une transmission à l'étranger et évoquer l'absence de dispositions appropriées en matière de protection des données. De plus, le consentement doit être librement donné, ce qui signifie que la personne concernée soit pouvoir se prononcer pour ou contre le traitement des données en dehors de toute pression¹¹⁵. Plusieurs auteurs affirment en outre qu'un consentement ne peut être libre que si la personne dispose d'une alternative non entachée d'inconvénients inacceptables¹¹⁶.

Dans le présent contexte, il est problématique que lors de traitements des données effectués sur la base d'injonctions de production, il n'y ait pas de lien entre la prestation que le CSP doit fournir au client et le traitement des données requis à cet effet. Le client devrait donc consentir à cette finalité non indispensable à la fourniture de la prestation afin de pouvoir prétendre à celle-ci. Si un contrat est subordonné au consentement à un traitement des données non indispensable à l'exécution du contrat, le droit européen présuppose que ce consentement n'a pas été librement donné. Pour les traitements de données effectués dans le cadre des poursuites pénales et de l'exécution des peines, on peut en outre partir du principe que la personne concernée n'a pas de véritable liberté de choix. Cela indique pour le moins que l'exigence d'un consentement juridiquement valable en rapport avec le *CLOUD Act* ne devrait pas être remplie, et un CSP ne pourrait invoquer le consentement de la personne concernée comme motif justificatif pour des traitements et des transmissions de données effectués sur la base d'injonctions de production.

Les responsables du traitement privés peuvent eux aussi invoquer un intérêt prépondérant privé ou public pour justifier un traitement des données portant atteinte à la personnalité. L'élément déterminant est cependant que dans le cadre d'une pesée des intérêts, les intérêts concernés soient mis en balance et que dans le résultat, l'intérêt privé ou public ait plus de poids que l'intérêt de la personne concernée par l'atteinte à la personnalité. L'art. 13, al. 2 LPD ou l'art. 31, al. 2 nLPD fournissent une liste (non exhaustive) de possibles intérêts prépondérants du responsable du traitement.

Outre les éventuels intérêts de tiers ou, à titre exceptionnel, l'intérêt de la personne concernée elle-même, l'*intérêt direct* du responsable du traitement peut justifier un traitement des données¹¹⁷. Dans le contexte de traitements des données effectués sur la base d'injonctions

¹¹⁴ BGE 136 II 508, consid. 5.2.4.

¹¹⁵ BAERISWYL, SHK DSG, art. 4, ch. 65.

¹¹⁶ Cf. RAMPINI dans BSK DSG, art. 13, ch. 6.

¹¹⁷ WERMELINGER, A., « Art. 13 », dans Baeriswyl, B. (Éditeur), *Datenschutzgesetz – Stämpfli's Handkommentar*, Berne : Stämpfli 2015, ch. 11.

Rapport sur le US CLOUD Act (loi *Cloud*)

de production, une justification dans l'intérêt propre du CSP devrait être examinée dans l'hypothèse où en cas de non-respect de l'injonction, il devrait s'attendre à des sanctions selon le droit américain. Ainsi, la Commission européenne, dans son « amicus brief » (requête) dans l'affaire Microsoft devant la Cour suprême des USA, a jugé possible, dans ce cas, un intérêt légitime du CSP. Mais même dans un contexte national, une conservation ou une transmission de données ne devrait être considérée comme licite que quand les intérêts de la personne concernée par l'atteinte à la personnalité ne sont pas prépondérants. Cependant, on ne peut s'attendre à ce qu'en cas de pesée des intérêts, un éventuel intérêt du CSP à ne pas être sanctionné serait prépondérant par rapport aux intérêts de la personne subissant l'atteinte à la personnalité. Cela revient à reconnaître que l'intérêt d'une personne à la protection de sa personnalité et de sa sphère privée et à l'autodétermination en matière d'information représente déjà *en soi* un intérêt de poids¹¹⁸. Dans la pesée des intérêts, il est probable que le fait que les USA offrent de moindres garanties en matière de protection des données ainsi que de moindres garanties procédurales pèse lui aussi lourdement dans la balance.

Comme exemples d'intérêts *publics* que des responsables du traitement privés peuvent faire valoir, on cite la sécurité ou la lutte contre le blanchiment d'argent¹¹⁹. Par intérêt public prépondérant, on entend ici l'intérêt public du point de vue de la Suisse. Ce dernier ne se limite pas exclusivement aux intérêts strictement nationaux ; au contraire, il peut aussi consister à soutenir les intérêts d'un pays étranger (par exemple dans la lutte contre le blanchiment d'argent), ou concerner les situations où les intérêts d'un pays étranger ont un « effet réflexe » sur la Suisse, et qu'il est donc, indirectement, dans l'intérêt de cette dernière de les soutenir¹²⁰. Un intérêt étranger en matière de lutte contre le terrorisme, par exemple, pourrait ainsi représenter un intérêt public justifié du point de vue de la Suisse¹²¹. Sur ce point, la Suisse semble moins restrictive que l'UE avec le RGPD, selon lequel il ne peut y avoir d'intérêt public que si celui-ci est reconnu dans le droit de l'Union ou dans celui d'un État membre.

Si l'infraction grave (*serious crime*) poursuivie concrètement au moyen d'une injonction de production était reconnue comme relevant de l'intérêt public, et qu'une transmission de données était indispensable à cet effet, un CSP traitant des données personnelles à cet égard pourrait invoquer ce motif justificatif. Cet intérêt public doit toutefois être prépondérant par rapport à l'intérêt de la personne concernée subissant l'atteinte à la personnalité. Cependant, les traitements de données effectués sur la base d'injonctions émanant des autorités américaines de poursuite pénale devant fondamentalement être considérés comme incompatibles avec les principes de protection des données en vigueur ici, la protection des droits de la personnalité, de la sphère privée et de l'autodétermination en matière d'information de la personne concernée devrait peser fortement dans la balance lors de l'évaluation. Il faudrait donc placer la barre très haut dans l'évaluation de la proportionnalité de tels traitements de données.

Enfin, le traitement des données peut aussi être justifié par la loi, seule une base juridique relevant du droit suisse pouvant être prise en considération comme motif justificatif d'une éventuelle atteinte à la personnalité. Étant donné que dans le présent contexte, c'est un acte juridique américain, à savoir le *CLOUD Act*, qui sert de base juridique aux injonctions, un CSP ne pourrait pas invoquer la loi comme motif justificatif du traitement selon l'art. 13, al. 1 LPD ou l'art. 31, al. 1 nLPD. Cette situation ne pourrait probablement changer qu'avec la conclusion avec les USA d'un traité global sur les échanges de données incluant des standards

¹¹⁸ ROSENTHAL, JÖHRI, art. 13, ch. 14 renvoie sur ce point à la jurisprudence du Tribunal fédéral, BGE 97 II 106 s.

¹¹⁹ MAURER-LAMBROU, STEINER, « Art. 6 LPD », ch. marg. 32.

¹²⁰ ROSENTHAL, JÖHRI, art. 6, ch. marg. 60. Aussi BAERISWYL, B., BLONSKI, D., « Art. 6 », dans Baeriswyl, B. (Éditeur), *Datenschutzgesetz – Stämpfli Handkommentar*, Berne : Stämpfli 2015, ch. marg. 30.

¹²¹ Cf. p. ex. ROSENTHAL, JÖHRI, art. 6, ch. marg. 61.

Rapport sur le US CLOUD Act (loi *Cloud*)

de protection correspondants, qui satisferait aux exigences en matière de communication transfrontière des données (art. 6, al. 2, let. a LPD ou art. 16, al. 2, let. a nLPD). Un simple *executive agreement* selon le *CLOUD Act* ne suffirait guère à satisfaire ces exigences.

5.5.2.4 Compatibilité avec les exigences relatives à la communication transfrontière de données (art. 6 LPD/art. 16 et 17 nLPD)

Après avoir été communiquées à l'étranger, les données personnelles ne sont plus protégées par la législation suisse en matière de protection des données, mais soumises à un ordre juridique étranger, ce qui accroît le risque d'atteintes à la personnalité. L'art. 6 LPD impose des conditions à de telles communications de données susceptibles de menacer gravement la personnalité des personnes concernées. Il faut supposer *ex lege* que c'est le cas lorsque le pays concerné ne dispose pas d'une législation assurant une protection des données adéquate, c'est-à-dire d'une protection comparable à celle garantie par le droit suisse. Pour les USA, ce n'est pas le cas. Ainsi, le PFPDT considère que le niveau de protection offert par les USA n'est *plus adéquat dans aucun domaine*.

Dans la mesure où il a été constaté plus haut que les traitements de données effectués sur la base d'injonctions de production étaient globalement problématiques au regard des principes de protection des données, et qu'il était probable qu'ils soient illicites au regard de la législation suisse en matière de protection des données, il est superflu d'examiner leur compatibilité avec les exigences relatives à la communication transfrontière de données.

Mais pour résumer, on peut retenir ceci : même en l'absence de protection adéquate à l'étranger, des communications de données peuvent être admises à titre exceptionnel, à savoir quand les instruments juridiquement contraignants et applicables prévoient des garanties appropriées pour protéger correctement les données à l'étranger, quand la personne concernée consent au transfert, quand la communication est indispensable soit à la sauvegarde d'un intérêt public prépondérant, soit à la constatation, l'exercice ou la défense d'un droit en justice, ou quand la communication est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers.

Concrètement, il serait envisageable que des CSPs communiquent des données personnelles aux autorités américaines de poursuite pénale dès lors que cela serait indispensable pour sauvegarder les intérêts vitaux de la personne concernée elle-même, ou pour défendre des droits en justice dans le cadre de procédures pénales concrètes en cours. En outre, des CSPs pourraient aussi invoquer des intérêts étrangers en matière de sécurité pour faire valoir un intérêt public du point de vue de la Suisse. Mais dans tous les cas, les intérêts concernés doivent être soigneusement mis en balance. Étant donné que par principe, il faut supposer que les droits de la personnalité des personnes dont les données personnelles ont été communiquées aux autorités américaines de poursuite pénale sur la base d'injonctions de production sont gravement menacés, ces situations exceptionnelles ne devraient être acceptées comme motifs justifiant de telles communications de données que dans de très rares cas.

5.5.2.5 Autres aspects problématiques du point de vue de la protection des données et de la protection des droits fondamentaux

On peut mentionner encore d'autres aspects problématiques du point de vue de la protection des données et de la protection des droits fondamentaux en lien avec de tels traitements de données. Au regard de la protection de la sphère privée (art. 13 Cst.), ces traitements de données doivent être considérés comme sensibles à divers égards. L'art. 8 de la Convention

Rapport sur le US CLOUD Act (loi *Cloud*)

européenne des droits de l'homme (CEDH)¹²² reconnaît le droit fondamental au respect de la vie privée. Selon la jurisprudence de la Cour européenne des droits de l'homme (CourEDH), toute ingérence dans la vie privée doit être prévue par la loi, poursuivre un but légitime et se limiter au nécessaire dans une société démocratique¹²³. En rapport avec le droit à la protection des données, la Cour utilise le critère de la « stricte nécessité »¹²⁴. Tant la CourEDH (appliquant en cela la CEDH) que la CJUE (appliquant en cela la Charte européenne) ont créé de nombreuses garanties relatives au contrôle des communications électroniques par les gouvernements¹²⁵.

Sous cet angle aussi, les aspects du *CLOUD Act* déjà évoqués au point 5.5.1.1 en rapport avec leur compatibilité au RGPD semblent problématiques¹²⁶. Il s'agit de la réglementation différente prévue par le *CLOUD Act* concernant les données liées ou non liées au contenu, et concernant les données des « *US Persons* » et des autres personnes ; de l'absence de distinction entre le responsable du traitement et le sous-traitant ; de la surveillance en temps réel du contenu des communications ; de l'absence de droits de la personne concernée, notamment le droit d'accès et d'information ; et de l'absence de voies de recours administratives et judiciaires pour la personne concernée. L'absence de droit à un jugement par un tribunal, déjà problématique au regard des prescriptions en matière de protection des données, est en outre incompatible, notamment, avec la garantie de l'accès au juge prévue par l'art. 29a Cst., selon lequel toute personne a droit à ce que sa cause soit jugée par une autorité judiciaire (en Suisse)¹²⁷.

5.5.2.6 Conclusion sur la compatibilité d'un *executive agreement* avec la protection des données

Dans l'ensemble, les communications et les traitements de données effectués sur la base d'injonctions de production doivent être considérés comme fondamentalement problématiques au regard non seulement de leur compatibilité avec le RGPD, mais aussi avec le droit suisse de la protection des données, et plus généralement du point de vue des droits fondamentaux. Enfin, une condition importante pour que le caractère adéquat du niveau de protection des données assuré par la Suisse soit reconnu par la Commission européenne est la ratification du Protocole d'amendement à la Convention sur la protection des données personnelles du Conseil de l'Europe (« Convention 108+ »)¹²⁸. La mise en œuvre, exigée par la Convention 108+, des mesures de protection des données prescrites étant une condition de sa ratification (art. 4, al. 2 Convention 108+), la conclusion d'un *executive agreement* doit être qualifiée de problématique à la lumière aussi de cette circonstance.

La protection des données n'étant pas suffisante aux USA, on peut poser pour acquis que des communications de données aux autorités américaines de poursuite pénale représenteraient une grave atteinte aux droits de la personnalité des personnes concernées. Sous réserve d'examen plus approfondi, on peut supposer que leur éventuel consentement ne représenterait probablement pas un motif justificatif valable. Il serait envisageable, certes,

¹²² RS 0.101

¹²³ Par exemple CourEDH, *Affaire Liberty et autres c. Royaume-Uni*, arrêt du 1^{er} juillet 2008, requête 58243/00, ECLI:CE:ECHR:2008:0701JUD005824300.

¹²⁴ CourEDH, *Szabó et Vissy c. Hongrie*, arrêt du 12 janvier 2016, requête 37138/14, ECLI:CE:ECHR:2016:0112JUD003713814, p. 33 ; CJUE, *Digital Rights Ireland et Seitlinger e. a.*

¹²⁵ CourEDH, *Roman Zakharov c. Russie*, arrêt du 4 décembre 2015, requête 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306.

¹²⁶ Voir le document « Évaluation du CCBE de la loi CLOUD Act des USA » du 28.02.2019, Conseil des Barreaux Européens, contenu disponible sur : https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_pers/FR_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf.

¹²⁷ Voir à ce sujet les explications figurant plus bas, point 5.6.1.

¹²⁸ RS 0.235.1

Rapport sur le US CLOUD Act (loi *Cloud*)

qu'un CSP puisse justifier un transfert de données par les intérêts sécuritaires des USA. Un autre motif justificatif envisageable serait que la communication soit effectuée dans l'intérêt de la personne concernée elle-même (c'est-à-dire pour sauvegarder ses intérêts vitaux ou pour défendre ses droits en justice dans le cadre d'une procédure pénale concrète). Mais même dans ce cas, lors de la pesée des intérêts, le fait que la communication de données menace gravement la personnalité des personnes concernées devrait peser lourd dans la balance.

Au regard des principes de protection des données que sont la transparence et la proportionnalité, notamment, les traitements de données effectués sur la base d'injonctions de production doivent être considérés comme problématiques. Même si, ici aussi, on ne pourrait exclure dans certains cas que les CSPs puissent invoquer un intérêt public digne de protection, ou les intérêts de la personne concernée elle-même, on peut s'attendre à ce qu'une violation des principes de protection des données, qui doit être considérée comme une atteinte grave aux droits de la personnalité de la personne concernée, ne puisse être justifiée que dans de très rares cas, conformément à la jurisprudence du Tribunal fédéral et à la position des autorités européennes de protection des données.

Même du point de vue d'autres exigences importantes pour la protection des données et la protection des droits fondamentaux, les traitements de données effectués sur la base d'injonctions de production se révèlent préoccupants. L'absence, dans le *CLOUD Act*, de droits d'accès, de rectification et de suppression des données de la personne concernée, pèse fortement dans la balance, de même que l'absence de possibilités de recours judiciaire et l'absence de garanties procédurales. Au regard notamment de la garantie de l'accès au juge prévue par l'art. 29a Cst., un *executive agreement* pose problème en droit suisse.

5.5.3 Quelle protection devrait être incluse dans un *executive agreement* avec les USA ?

Un éventuel *executive agreement* serait un accord international conclu entre la Suisse et les USA. Cet accord devrait comporter des garanties suffisantes pour que les standards de protection des données et de protection des droits fondamentaux correspondants au droit suisse soient garantis, y compris pour les données personnelles devant être communiquées aux autorités américaines de poursuite pénale. Faute de garanties correspondantes dans le *CLOUD Act*, les garanties et principes essentiels ainsi que les droits des personnes concernées devraient être réglés dans l'accord lui-même.

Ceci étant, on peut se demander si le cadre prescrit par le *CLOUD Act* pour les *executive agreements* permet d'offrir de telles garanties globales en matière de protection des données, notamment parce que cette loi elle-même pose des problèmes du point de vue de la protection des données. Il faut en particulier évoquer le fait que même s'il existait un tel *executive agreement*, une personne concernée n'aurait pas la possibilité de s'opposer à la communication de ses données personnelles puisque le seul mécanisme d'opposition prévu par le *CLOUD Act* ne concerne que les CSPs, et qu'il est d'ailleurs extrêmement limité. Les négociations en cours entre l'UE et les USA (voir le chiffre 4.2.2) témoignent de l'intention de l'UE de régler les échanges de preuves électroniques en matière pénale par un accord-cadre global dont la substance irait bien au-delà de celle d'un *executive agreement*.

La décision de la Commission européenne du 28 juin 2021 concernant le caractère adéquat du niveau de protection des données personnelles assuré par le Royaume-Uni selon le RGPD montre que la conclusion d'un *executive agreement* avec les USA aura des conséquences sur l'évaluation future du caractère adéquat de la protection des données assurée par la Suisse. La décision du Parlement européen du 21 mai 2021 de rejeter la décision

Rapport sur le US CLOUD Act (loi *Cloud*)

d'adéquation concernant le Royaume-Uni présentée par la Commission (décision motivée, entre autres, par la référence aux « onward transfers of data to other countries and bulk access to data by law enforcement »¹²⁹) révèle le bien-fondé de cette supposition.

À la différence du Royaume-Uni, qui contrairement à la Suisse applique intégralement le RGPD, hormis dans le domaine du contrôle de l'immigration, et qui promet d'imposer dans l'accord bilatéral conclu entre le Royaume-Uni et les USA sur la base du *CLOUD Act* une référence aux droits et garanties figurant dans l'accord-cadre entre l'UE et les USA, il faut supposer qu'un *executive agreement* que la Suisse conclurait avec les USA dans le cadre étroit du *CLOUD Act* ne suffirait pas à garantir le niveau de protection adéquat que l'UE exige. À cet égard, et en conformité avec les négociations entre l'UE et les USA, il faudrait plutôt viser un accord global qui réglerait intégralement les traitements et les communications de preuves électroniques en matière pénale par les CSPs aux autorités américaines et suisses de poursuite pénale, et garantirait un niveau élevé de protection des données personnelles traitées dans ce cadre et des libertés et droits fondamentaux des personnes concernées. Compte tenu de ce qui précède, il est dans l'intérêt de la Suisse d'attendre les résultats des négociations entre l'UE et les USA sur le futur accord.

Par ailleurs, il convient de suivre les évolutions actuelles au niveau européen dans le domaine de la protection des données. Dans son arrêt du 16 juillet 2020 concernant l'affaire « Schrems II », la CJUE note que les dispositions relatives aux programmes de surveillance n'offrent, dans le droit américain, pas de garanties suffisantes de respect des exigences du RGPD en matière de protection des données, ni de possibilités de recours suffisantes pour les personnes concernées qui ne sont pas américaines¹³⁰. Dans ses décisions concernant le caractère adéquat du niveau de protection des données assuré par le Royaume-Uni, la Commission européenne s'appuie pour l'essentiel sur cette décision. De ce fait, il est probable qu'elle ait une influence majeure sur l'appréciation d'un éventuel *agreement* avec les USA sous l'angle de l'adéquation du niveau de protection des données assuré par la Suisse. De même, la mise en conformité des actes juridiques européens régissant les traitements de données dans le domaine des poursuites pénales et de l'exécution des peines avec la directive (UE) 2016/680 permet de supposer qu'à l'avenir, les communications de données depuis l'UE vers des pays tiers seront évaluées selon des critères encore plus stricts¹³¹.

5.6 Compatibilité avec le droit suisse d'entraide judiciaire

L'entraide internationale en matière pénale (entraide judiciaire accessoire) entre la Suisse et les USA est essentiellement régie par le TEJUS, ainsi que par la loi fédérale du 3 octobre 1975 relative à ce traité (LTEJUS)¹³². Les aspects non réglementés dans le TEJUS et la LTEJUS sont couverts par l'EIMP et son ordonnance d'application (OEIMP)¹³³, tandis que le code de procédure pénale (CPP)¹³⁴ s'applique aux mesures dont ne traite pas directement l'EIMP. Par ailleurs, les CSPs suisses sont soumis à la LSCPT.

¹²⁹ Voir le communiqué de presse du Parlement européen du 21.5.2021, consultable à l'adresse : <https://www.europarl.europa.eu/news/en/press-room/20210517IPR04124/data-protection-meps-urge-the-commission-to-amend-uk-adequacy-decisions> (version du 26.5.2021).

¹³⁰ CJUE, *Schrems II*, consid. 175-178.

¹³¹ Communication de la Commission au Parlement européen et au Conseil - Marche à suivre en ce qui concerne la mise en conformité de l'acquis de l'ancien troisième pilier avec les règles en matière de protection des données, consultable à l'adresse : https://ec.europa.eu/info/sites/default/files/1_fr_act_part1_v1_0.pdf (version du 1^{er}.7.2020).

¹³² RS 351.93

¹³³ RS 351.11

¹³⁴ RS 312.0

Il convient donc d'examiner la compatibilité du *CLOUD Act* et d'un éventuel *executive agreement* avec les bases légales précitées, sachant que l'ensemble des mesures déployées en matière de preuves électroniques bousculent clairement le cadre traditionnel de l'entraide judiciaire. Au vu des textes juridiques, cela est inévitable et tout à fait intentionnel. Cette partie explicitera néanmoins ce « changement de paradigme » – qui s'éloigne de l'entraide classique pour s'orienter vers une forme de coopération plus directe – sous l'angle des principes du droit suisse de l'entraide judiciaire et s'attachera à déterminer les possibilités et les limites qui ressortent de ces principes.

5.6.1 Motifs de refus d'une requête d'entraide judiciaire et garantie de recours judiciaire

La procédure d'entraide judiciaire suisse soumet la recevabilité des requêtes émanant d'un gouvernement étranger à certaines conditions. Les autorités doivent d'office vérifier si elles sont remplies lorsque la recherche des preuves a lieu en Suisse, et les personnes concernées peuvent s'en prévaloir dans le cadre d'une procédure devant les autorités et les tribunaux suisses. Les principaux motifs d'irrecevabilité des requêtes d'entraide judiciaire sont énumérés aux art. 2 et 3 EIMP¹³⁵. Ainsi, aucune entraide n'est accordée pour les délits à caractère politique, militaire, fiscal¹³⁶, monétaire, commercial ou économique. Il en va de même lorsque les requêtes étrangères enfreignent les principes de procédure élémentaires et présentent de graves défauts. C'est par exemple le cas lorsque la procédure à l'étranger n'est pas conforme aux principes de la CEDH, lorsqu'elle tend à punir la personne poursuivie en raison de ses opinions politiques, de son appartenance à un groupe social déterminé, de sa race, de sa confession ou de sa nationalité, ou lorsque l'entraide risque d'aggraver la situation de la personne poursuivie pour l'une ou l'autre des raisons évoquées.

Les motifs d'irrecevabilité se fondent sur l'art. 5 Cst., qui dispose que l'activité de l'État doit toujours être conforme au droit, y compris au droit international. Un *executive agreement* autoriserait un CSP domicilié en Suisse à participer directement à une procédure pénale engagée par l'administration américaine ; les informations et les preuves (numériques) ne seraient plus collectées par l'administration suisse dans le cadre d'une procédure administrative suisse. En fournissant des données relatives à des personnes tierces (ses clients) dans le cadre d'une procédure pénale étrangère susceptible de les utiliser comme preuves, le CSP accomplirait de facto une tâche régalienne. L'*executive agreement* déléguerait donc à une personne privée, le CSP, une tâche relevant en droit suisse de la souveraineté nationale. De ce fait, le CSP resterait lié par les droits fondamentaux. Par conséquent, un *executive agreement* ne devrait pas porter atteinte au niveau de protection garanti par les libertés fondamentales, lequel correspond au niveau de protection prévu par le droit d'entraide actuel.

La Suisse devrait donc impérativement mettre en place une procédure nouvelle et directe, qui permette de faire valoir ces motifs de refus dans le cadre du *CLOUD Act*. Il ne s'agit rien de moins que de garantir l'ordre public¹³⁷, notamment pour les délits politiques et fiscaux. Les motifs de refus devraient probablement aussi être inscrits dans un éventuel *executive agreement* entre la Suisse et les USA. La Suisse devant également être en mesure de respecter les garanties minimales prévues par la CEDH, celles-ci devraient donc aussi figurer en détail dans l'*executive agreement*.

¹³⁵ Ces motifs figurent également dans les traités bilatéraux d'entraide judiciaire récents signés par la Suisse, ainsi que dans la clause d'exclusion discrétionnaire de l'ancienne version du TEJUS, dont la rédaction volontairement non explicite évoque « d'importants intérêts de nature similaire » (art. 3, al. 1, let. a).

¹³⁶ Sauf, par exception, dans les cas d'escroquerie fiscale, cf. art. 3, al. 3, EIMP.

¹³⁷ ZIMMERMANN, ch. marg. 612.

Rapport sur le US CLOUD Act (loi *Cloud*)

Dès lors, il se pose la question de savoir quelle procédure permettrait de garantir ces motifs de refus, car le *CLOUD Act* n'accorde aucune compétence aux autorités suisses, ni ne s'appuie sur une procédure suisse. Seul le CSP dispose de voies de recours contre la procédure américaine, devant un tribunal américain, et peut contester l'utilisation des données s'il estime qu'elle enfreint les lois suisses en vigueur. La Suisse n'a encore jamais accepté une allégeance aussi inconditionnelle à une législation ou à des tribunaux étrangers. Par ailleurs, la conformité constitutionnelle d'une procédure de cette nature, résultant d'un *executive agreement*, est très hypothétique, surtout au regard de la garantie de l'accès au juge prévue par l'art. 29a Cst. Un cadre d'une autre nature que celui prévu par un *executive agreement* assujéti au *CLOUD Act* serait donc très probablement nécessaire, comme évoqué dans la partie sur la protection des données.

5.6.2 Principe de la double incrimination

Le principe de la double incrimination autorise le recours à une mesure de contrainte pour satisfaire à l'obligation d'entraide judiciaire entre pays à la condition que les faits commis soient passibles de poursuites pénales aussi bien dans l'État requérant que dans l'État coopérant. Or le *CLOUD Act* ne prévoit aucune mesure de contrainte. La notion de *serious crime* définie dans l'*executive agreement* signé par le Royaume-Uni et les USA sur la base de la peine privative de liberté encourue est censée limiter la coopération sur la base du *CLOUD Act* aux délits le plus graves, mais l'accord en question ne subordonne pas l'entraide judiciaire au principe de la double incrimination. Des voix se sont élevées à plusieurs reprises pour critiquer ce point¹³⁸, car, cela signifie que tout délit punissable d'au moins trois ans de prison aux USA peut donner lieu à une injonction de production à l'intention d'un CSP domicilié au Royaume-Uni, et que ce dernier a l'obligation d'y répondre même si le délit en question n'est pas passible de sanctions pénales au Royaume-Uni. Dans le cadre d'un éventuel *executive agreement*, ce point pourrait se révéler particulièrement délicat pour la Suisse, notamment en matière de délit fiscal.

Compte tenu du principe connu de la double incrimination en matière de coopération internationale, il se pose la question de savoir si la Suisse pourrait, sur la base du *CLOUD Act*, envisager de répondre à une requête d'entraide judiciaire pour des faits ne présentant aucun caractère pénal sur son territoire. Si la réponse est négative, il faudrait ajouter le critère de la double incrimination à la notion de *serious crime* (infraction grave) dans l'*executive agreement*. Ce qui, de nouveau, ferait resurgir la question de savoir comment la conformité à ces conditions pourrait être vérifiée en l'absence de toute procédure suisse et, au besoin, de savoir comment elle pourrait être imposée. Le fait de savoir s'il suffit ou pas que le CSP – qui, rappelons-le, n'est pas la personne faisant l'objet de l'enquête – pourrait faire valoir dans une procédure pénale aux USA le fait que le délit fiscal incriminé ne rentre pas dans le champ d'application de l'entraide judiciaire en Suisse est une question de nature politique.

5.6.3 Droit d'être entendu

La question du droit à être entendu renvoie elle aussi à la Constitution dans la mesure où l'art. 29, al. 2 Cst. garantit aux parties le droit d'être entendues. Toute personne a donc le droit de présenter ses arguments, d'avoir accès à son dossier, de fournir ou de demander des preuves sur des faits susceptibles d'influer sur la décision finale, d'être associée à l'obtention desdites preuves, ainsi que de les consulter et de prendre position à leur égard pour empêcher qu'une décision lui portant injustement préjudice ne soit prise.

¹³⁸ Celle de l'ONG Human Rights Watch par exemple, dont la lettre ouverte est disponible sur Internet: <https://www.hrw.org/news/2019/10/29/groups-urge-congress-oppose-us-uk-cloud-act-agreement>.

Rapport sur le US CLOUD Act (loi *Cloud*)

En matière de coopération pénale internationale, ces obligations résultent des art. 29 ss PA ainsi que de certaines dispositions spécifiques de l'EIMP et de la LTEJUS.

L'actuelle procédure d'entraide judiciaire avec les USA prévoit que la personne mise en cause a le droit de se faire assister d'un mandataire (art. 21 EIMP), de consulter les pièces de son dossier (art. 26 et 27 PA par référence à l'art. 9 LTEJUS) et de participer à l'exécution de la demande (art. 12, al. 2 et art. 18, al. 1 TEJUS), le droit de toute personne personnellement et directement touchée par une mesure d'entraide et ayant un intérêt digne de protection à ce qu'elle soit annulée ou modifiée de se voir notifier une décision motivée lui permettant de faire valoir son droit de recours (art. 17 s. LTEJUS) ainsi que le droit d'être informée sur lesdites voies de recours (art. 22 EIMP).

Le *CLOUD Act* permettrait à l'autorité compétente en Suisse (définie dans l'*executive agreement*) de demander directement aux CSPs ayant leur siège aux USA des informations et des données enregistrées sur leurs serveurs et, inversement, les autorités américaines pourraient directement demander aux CSPs ayant leur siège en Suisse des données stockées sur leurs serveurs. Ce système aboutirait à une situation où ni les personnes (physiques et morales) dont les données seraient requises, ni une autre autorité (par exemple l'OFJ en tant qu'autorité de surveillance ou autorité centrale), ne se verraient averties du transfert de données et informations. Elles ne pourraient donc pas demander activement à être prévenues du transfert de leurs données¹³⁹ ni s'exprimer à propos dudit transfert. Par conséquent, le droit d'être entendu de la personne ou de l'autorité directement concernée par la divulgation d'informations ne pourrait pas être garanti.

Le *CLOUD Act* ne reconnaissant pas le droit d'être entendu de la personne ou de l'autorité concernée, il convient de se demander si ce droit pourrait être inscrit dans un *executive agreement*. Dans le cas d'une réponse positive, il faut de nouveau se poser la question de savoir si ce droit pourrait être garanti en l'absence de toute procédure en Suisse. Dès lors, un *executive agreement* serait difficilement compatible avec l'exigence constitutionnelle posée par l'art. 29., al. 2 Cst. Le cadre du traité devrait donc être élargi.

5.6.4 Autorité de surveillance et de contrôle

L'OFJ est, au premier chef, l'autorité chargée de l'exécution des traités et de la législation fédérale en matière de coopération pénale internationale (art. 17, al. 2 EIMP et art. 7, al. 6a de l'ordonnance du 17 novembre 1999 sur l'organisation du Département fédéral de justice et police, Org DFJP)¹⁴⁰. Dans le domaine de l'entraide pénale internationale avec les USA, il exerce à la fois la fonction d'autorité centrale instituée par l'art. 28, al. 1 TEJUS et la fonction d'autorité de surveillance qui lui revient (art. 19, al. 1, première phrase LTEJUS) en raison de sa qualité pour recourir contre les décisions de l'autorité cantonale ou fédérale d'exécution. Il est également fondé à recourir devant le Tribunal fédéral contre les décisions du Tribunal pénal fédéral (art. 19, al. 1, première phrase LTEJUS).

En plus de la possibilité de déposer un recours, l'OFJ exerce son devoir de surveillance sur toute la procédure d'entraide en Suisse, notamment lorsqu'il vérifie si les conditions de recevabilité d'une requête d'entraide sont remplies, si les décisions prises par les autorités d'exécution (notamment les ministères publics cantonaux et le Ministère public de la Confédération) respectent les dispositions du droit d'entraide et lorsqu'il transmet les informations et les

¹³⁹ En vertu de l'art. 3, al. 1, let. a, ch. 3 de la loi fédérale sur le principe de la transparence dans l'administration (LTrans, RS 152.3), les procédures d'entraide judiciaire et administrative internationale sont exclues du champ d'application de la loi. L'accès aux documents relèverait donc des seules dispositions de l'*executive agreement*.

¹⁴⁰ RS 172.213.1

Rapport sur le US CLOUD Act (loi *Cloud*)

moyens de preuve en précisant l'emploi qui peut en être fait par l'autorité requérante selon le principe de spécialité (art. 5 TEJU). L'OFJ contrôle également les requêtes d'entraide adressées aux États étrangers (art. 30 EIMP).

Le *CLOUD Act* permet aux autorités suisses désignées de demander directement des données aux CSPs américains, et aux autorités américaines de faire de même avec les CSPs suisses. Les CSPs suisses recevraient ainsi des injonctions de production dont l'OFJ n'aurait très probablement pas connaissance et sur lesquels il ne serait donc pas à même d'exercer son devoir de surveillance. En outre, l'autorité définie dans l'*executive agreement* comme autorité compétente pour établir des injonctions de production en Suisse serait toute à la fois autorité d'exécution et seule garante du respect du droit.

Le *CLOUD Act* attribue aux CSPs un rôle clé pour les requêtes déposées par les USA. Ils seraient seuls à avoir connaissance d'une demande et auraient le contrôle sur la procédure en découlant¹⁴¹. Les prestataires de petite taille pourraient manquer d'expertise et de ressources pour assumer ce rôle¹⁴². Pour les requêtes déposées par la Suisse, ce rôle serait endossé par les autorités d'exécution.

Bien qu'une injonction de production soit censée être soumise à un certain contrôle¹⁴³, le *CLOUD Act* ne semble pas prévoir l'institution d'une autorité de surveillance en tant que telle. L'un de ses buts semblant être l'immédiateté et la rapidité de l'échange d'informations et de données, un mécanisme de surveillance ralentirait effectivement le processus. Toutefois, la possibilité d'instaurer un mécanisme de contrôle limité dans un *executive agreement* ne semble pas exclue, comme le montre l'accord conclu entre le Royaume-Uni et les USA. (cf. ci-dessus chiffre 4.1).

Il convient donc de se demander si – contrairement au concept du *CLOUD Act* – une autorité de surveillance ou de contrôle pourrait être instituée dans le cadre d'un *executive agreement*, tant pour les requêtes d'entraide adressées à la Suisse que pour celles qu'elle dépose. Cela serait probablement la seule façon de garantir la constitutionnalité de l'entraide internationale (cf. ci-dessous chiffre 5.6.8.). Reste à définir la place que tiendrait cette autorité de surveillance, ainsi que les rôles et les possibilités concrètes de contrôle qui seraient les siens.

5.6.5 Principe de spécialité

Dans le domaine de l'entraide, le principe de spécialité interdit l'utilisation par l'État requérant des documents, renseignements et informations reçus dans une procédure visant des délits pour lesquels l'entraide est exclue en Suisse. Cela concerne les infractions politiques, militaires, fiscaux¹⁴⁴, monétaires et économiques ou les cas dans lesquels l'octroi de la coopération compromettrait la souveraineté, la sûreté, l'ordre public ou d'autres intérêts essentiels de l'État à qui la requête est adressée¹⁴⁵. Le principe de spécialité protège aussi bien la souveraineté de la Suisse que la personne visée par les actes d'entraide. Le principe de spécialité s'impose à l'État requérant, ainsi qu'à tout État tiers qui pourrait avoir ultérieurement connaissance des renseignements par son entremise.

¹⁴¹ Cf. BISMUTH, p. 685.

¹⁴² BISMUTH, p. 685.

¹⁴³ *CLOUD Act*, § 2523 (b) (3) (D) (v).

¹⁴⁴ L'entraide est autorisée pour les escroqueries fiscales, cf. art. 3, al. 3 EIMP.

¹⁴⁵ Cf. l'art. 2 de la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 (CEEJ, RS 0.351.1) ainsi que l'art. 1a et l'art. 3 EIMP.

Rapport sur le US CLOUD Act (loi *Cloud*)

Le principe de spécialité s'applique aussi aux relations avec les USA¹⁴⁶. Même si les entités gouvernementales fondées par un *executive agreement* à demander des données au sens de l'accord devaient avoir un mandat clairement défini juridiquement ainsi que des procédures transparentes, notamment en ce qui concerne l'utilisation des données¹⁴⁷, le *CLOUD Act* ne semble contenir aucune clause s'apparentant au « principe de spécialité », ou du moins aucune réglementation claire et effective qui autoriserait ou interdirait l'utilisation des données reçues.

L'accord entre le Royaume-Uni et les USA reprend une possibilité déjà prévue dans le *CLOUD Act*: les données obtenues sur la base de l'accord ne peuvent être transmises à un État tiers sans le consentement de l'État dans lequel le CSP a son siège (art. 8, al. 2). L'accord prévoit également que l'État tiers doit être informé lorsque la personne dont les informations sont demandées ne se trouve pas au Royaume-Uni ou n'est pas un ressortissant américain¹⁴⁸. Si les données concernent des crimes qui pourraient mener à la peine de mort aux USA ou à la violation de la liberté d'expression au Royaume-Uni, l'autorité centrale de l'autre État doit être informée et donner son accord (art. 8, al. 4). Comme mentionné au point 4.1, les données obtenues sur la base du *CLOUD Act* ne peuvent être utilisées pour prononcer une peine de mort aux USA ou pour violer la liberté d'expression au Royaume-Uni sans l'accord préalable de l'autre État. Le Royaume-Uni a donc un droit de veto en ce qui concerne l'utilisation des preuves obtenues dans les affaires où la peine de mort est requise.

Dans le cadre d'un *executive agreement*, le contrôle de l'utilisation des données transmises échapperait largement à la Suisse, et plus encore si aucune autorité de surveillance puissante (au sens large) n'était instituée par cet accord. La question se pose donc de savoir si le principe de spécialité tel qu'il est pratiqué aujourd'hui (avec l'exception des délits fiscaux par exemple) pourrait être inscrit dans un *executive agreement*. Mais avant tout, il faut s'interroger sur ses modalités d'application : comment les définir pour qu'elles soient suffisamment conciliables avec les règles de droit suisse de rang supérieur, et de surcroît dans une procédure exclusivement américaine et où la seule partie appliquant ces règles serait le CSP concerné ?

5.6.6 Limitation de la coopération internationale pour motifs politiques

Il a été mentionné plus haut que la Suisse pouvait refuser l'entraide judiciaire si la demande était susceptible de porter atteinte à la souveraineté, à la sûreté, à l'ordre public ou à d'autres intérêts essentiels de l'État¹⁴⁹. Généralement, une telle situation survient à la suite d'une réclamation de la partie concernée. Lorsque de tels intérêts sont en jeu, l'entraide judiciaire peut également être assortie de conditions¹⁵⁰. Dans ce cas, la décision relève de la compétence du DFJP, qui prend l'avis des autres départements. La décision du DFJP peut donner lieu à un recours au Conseil fédéral. Une telle « clause de protection de la souveraineté » serait difficilement compatible avec le *CLOUD Act*.

¹⁴⁶ Cf. art. 5, al. 1 TEJUS et art. 67 EIMP. Pour les réserves, cf. ZIMMERMANN, ch. marg. 734 avec commentaires supplémentaires.

¹⁴⁷ *CLOUD Act*, § 2523 (b) (1) (B) (iv)

¹⁴⁸ Art. 5 de l'accord. Cf. également DASKAL, SWIRE, « The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards » ; dans ce contexte, l'État tiers est l'État dont la personne concernée possède la nationalité.

¹⁴⁹ Art. 1a EIMP ; cf. aussi art. 3, al. 1, let. a TEJUS.

¹⁵⁰ ZIMMERMANN, ch. marg. 714.

5.6.7 Compatibilité avec le code de procédure pénale et la loi fédérale sur la surveillance de la correspondance par poste et télécommunication

La rédaction des dispositions d'un éventuel accord bilatéral devrait également se conformer aux règles en vigueur du CPP¹⁵¹ et des actes législatifs en matière de procédure pénale, ainsi qu'à la LSCPT¹⁵². Il faudrait impérativement veiller à ce que les autorités étrangères ne se voient pas accorder des pouvoirs et des possibilités plus étendus que les autorités nationales. Cela signifie par exemple que les autorités américaines de poursuite pénale ne pourraient pas émettre d'injonctions de production (transfrontières) de plus large portée que les autorités pénales suisses vis-à-vis des CSPs domiciliés en Suisse, ou que la protection légale concernant les injonctions de production américaines ne devrait pas être moindre que celle qui concerne les mesures nationales¹⁵³.

Au vu du système mis en place par le *CLOUD Act*, cet impératif ne va pas sans difficultés. Les exigences du CPP et de la LSCPT devraient s'appliquer dans les procédures américaines, y compris pour les découvertes fortuites (art. 243 et 278 CPP), l'interdiction d'exploiter les preuves, etc., car il n'y aurait plus de procédure suisse.

La procédure inscrite dans le *CLOUD Act* pourrait difficilement être réglementée dans un *executive agreement* d'une manière qui correspondrait en Suisse aux bases légales précitées. Si une autorité suisse assumait une fonction de surveillance en tant qu'autorité centrale pour la collecte de données par les USA, elle effectuerait un contrôle préliminaire et pourrait rappeler le principe de spécialité lors de l'envoi des données. Mais même ainsi le respect des exigences aux procédures nationales ne serait pas garanti. Il est ainsi difficilement envisageable qu'un droit de recours suffisamment large puisse être instauré dans ce cadre.

Dès lors, il convient de se demander si les principales dispositions en vigueur afférentes à la transmission transfrontière de preuves électroniques ne devraient pas plutôt faire l'objet d'une loi nationale. Une telle loi pourrait servir de base légale pour un nombre infini d'accords bilatéraux. C'est la voie adoptée par le Royaume-Uni et l'Australie. Un tel système permettrait d'instaurer un socle de compatibilité par voie législative, mais laisserait tout de même subsister des questions de droit pour l'*executive agreement* qui serait conclu sur sa base. Il faudrait ainsi commencer par définir les liens concrets entre les différents ordres juridiques et, en plus, préciser toute une série d'aspects techniques, comme la question des délais de conservation des données secondaires ou leur application aux CSPs américains. Le droit suisse prévoit par exemple un délai de conservation ainsi qu'une durée pour la surveillance rétroactive, ce qui ne semble pas être le cas des USA. Qu'en serait-il dans l'accord bilatéral ?

¹⁵¹ Principales conditions posées par le CP pour la surveillance de la correspondance par poste et télécommunication : ordonnance de la surveillance par le ministère public (art. 269, al. 1, phrase introductive ; art. 273, al. 1 CPP) ; graves soupçons laissant présumer une des infractions énumérées à l'art. 269, al. 2 CPP pour la surveillance du contenu des télécommunications (art. 269, al. 1, let. a CPP) ou un crime, un délit ou une contravention au sens de l'art. 179^{septies} CP pour la surveillance des données secondaires (art. 273, al. 1 CPP) ; gravité de l'infraction justifiant la surveillance (respect du principe de la proportionnalité : art. 269, al. 1, let. b. CPP) ; respect du principe de la subsidiarité (art. 269, al. 1, let. c. CPP) ; autorisation par le tribunal des mesures de contrainte (art. 272, al. 1 et art. 273, al. 2 CPP) ; gestion des informations non nécessaires (art. 276 CPP) ; recevabilité des informations recueillies lors d'une surveillance non autorisée (art. 277 CPP) ; règles pour les découvertes fortuites (art. 278 CPP) ; communication de la surveillance (art. 279, al. 1 et 2 CPP) ; recours (art. 279, al. 3 CPP).

¹⁵² Les principales conditions posées par la LSCPT pour la surveillance de la correspondance par poste et télécommunication sont : le service chargé de la surveillance de la correspondance par poste et télécommunication constitue pour ainsi dire l'interface entre les autorités de poursuite pénale et l'opérateur (l'injonction de surveiller n'est pas directement communiquée par les autorités pénales à l'opérateur ; elle est d'abord transmise au Service SCPT qui le transmet lui-même à l'opérateur en vertu d'une décision y afférente [art. 5 PA] ; les données communiquées par l'opérateur ne sont pas directement transmises aux autorités de poursuite pénale, mais au Service SCPT, qui ensuite les communique au service pénale compétent ; obligations spécifiques de différentes catégories d'opérateurs, citées dans la loi ou les ordonnances y relatives, obligations plus ou moins larges selon la nature de l'opérateur ; rémunération de l'opérateur pour chaque surveillance versée par le Service SCPT et financé en partie par ledit service et en partie par l'autorité de poursuite pénale ; recours de l'opérateur contre la décision administrative du Service SCPT (aucune réclamation ne peut être déposée dans le cadre d'une procédure de droit pénal).

¹⁵³ Cf. p. ex. art. 274 et 279 CPP.

5.6.8 Quels contenus « juridiques d'entraide judiciaire » devraient figurer dans un *executive agreement* ?

Même si la Suisse conclutait un *executive agreement*, elle resterait soumise à ses obligations en matière de droits humains et de libertés fondamentales. Du point de vue juridique, il faudrait donc impérativement trouver les moyens de garantir le respect des droits constitutionnels tels que le *droit d'être entendu* (art. 29, al. 2 Cst.) et la *garantie de l'accès au juge* (art. 29a Cst.). Le respect des *garanties minimales de la CEDH* ainsi que de l'ordre public suisse (notamment en cas d'exclusion de l'entraide judiciaire dans le domaine des délits politiques ou fiscaux) doit également être garanti. Il faut également s'assurer qu'un éventuel *executive agreement* ne privilégie pas de manière exagérée les autorités de poursuite pénale américaines par rapport aux autorités de poursuite pénale suisses, en ce qui concerne la collecte des données en Suisse (cf. point 5.4.3.). Il est difficile d'imaginer comment toutes les dispositions du *code de procédure pénale suisse* pourraient être ancrées dans un *executive agreement*. Il est donc indispensable que la Suisse définisse d'abord ses propres standards en matière de production transfrontière de preuves électroniques (système *e-evidence*), avant de coopérer dans ce domaine avec les États partenaires dans le cadre de traités. En outre, cela permettrait de concevoir ce système de manière autonome et en tenant compte du droit suisse, de sorte que la souveraineté de la Suisse serait suffisamment garantie et nos valeurs fondamentales préservées, même en cas de collaboration directe dans le domaine des preuves électroniques.

6 Sécurité des données et décryptage

6.1 Transmission sécurisée

Le transfert de données d'un CSP suisse vers une autorité de poursuite pénale américaine doit être conforme à la législation suisse. En l'espèce, il faut vérifier comment les données personnelles sont transférées d'un CSP à une autorité étrangère. Pour les systèmes de messageries électroniques (ou les autres avec des serveurs intermédiaires), un cryptage du contenu et du transfert est nécessaire pour garantir la protection des données pendant tout le transfert. Pour une plateforme de téléchargement (ou un système similaire sans transmission de données à d'autres systèmes), le cryptage du transfert semble suffisant si la plateforme est gérée par l'autorité elle-même. Si la plateforme de téléchargement de l'entreprise est externalisée, un cryptage du contenu est à nouveau nécessaire.

Si des données particulièrement sensibles devaient être transférées, ce qui est en général le cas dans le cadre de procédures pénales, le guide relatif aux mesures techniques et organisationnelles de la protection des données du PFPDT prévoit le cryptage permanent des données personnelles¹⁵⁴.

Un *executive agreement* devrait donc également contenir des dispositions qui garantissent le respect de ces règles de transmission des données à une autorité de poursuite pénale américaine. Par conséquent, les résultats des négociations entre les USA et l'UE devraient être utiles pour la Suisse.

¹⁵⁴ PFPDT, guide relatif aux mesures techniques et organisationnelles de la protection des données, août 2015, p. 20, disponible sur : <https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/datenschutz/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html>.

6.2 Cryptage neutre

La conservation des données sous une forme cryptée *chez le* CSP pose problème en ce qui concerne la question de la transmission légale et sécurisée des données d'un CSP suisse aux autorités de poursuite pénale américaines ou inversement.

Les CSPs peuvent proposer une multitude de prestations de services conformes aux exigences relatives à la sécurité des données (des clients). Les cryptages en font partie. Le *CLOUD Act* n'impose pas de décrypter les données. Il ne contient en particulier aucune disposition relative au décryptage des données dont disposent les CSPs pour le compte de leurs utilisateurs¹⁵⁵. Les CSPs ne peuvent donc pas être contraints de décrypter les données qui ont été cryptées par les clients¹⁵⁶.

Dans des dispositions légales spéciales (p. ex. art. 12, al. 5 de l'ordonnance sur le dossier électronique du patient [ODEP])¹⁵⁷, la FINMA ou l'OFSP ont certes imposé la conservation des données des clients en Suisse et selon le droit suisse. Même si les personnes concernées, à savoir ici les fournisseurs de prestations financières et médicales, respectent cette obligation en conservant des données particulièrement sensibles dans des datacenters suisses, les autorités américaines peuvent avoir accès aux données dans certaines situations relevant du champ d'application du *CLOUD Act*. Lors du transfert des données, des devoirs de discrétion légaux et/ou contractuels peuvent exiger que les données soient conservées sous une forme cryptée. Lors du cryptage, il existe diverses procédures techniques qui diffèrent notamment selon qu'elles prévoient ou non la possibilité d'accéder aux données par des moyens techniques en vertu du *CLOUD Act*.

Il convient d'abord de faire une distinction entre le cryptage côté client et le cryptage côté serveur. Lorsque les données sont déjà cryptées sur l'ordinateur du client ou du propriétaire des données, puis transmises au CSP sous cette forme (cryptage côté client), la clé de chiffrement reste chez le client. Le CSP ne peut pas décrypter les données. Par conséquent, celles-ci sont protégées contre un accès des autorités américaines dans le cadre du *CLOUD Act*, sans que le client ou le propriétaire des données ait à intervenir. La situation est différente en cas de cryptage côté serveur. Il faut faire une distinction entre trois variantes. Dans la première variante, la gestion de la clé de chiffrement est confiée au CSP qui la conserve sur le cloud et y a accès de manière légale. En principe, le CSP peut permettre aux autorités américaines d'avoir accès aux données cryptées. La protection des données des clients dépend de la volonté de coopération du CSP car, tel que mentionné ci-dessus, le CSP n'est pas tenu de décrypter les données des clients conformément au *CLOUD Act*. Dans la deuxième variante, le client gère seul la clé de chiffrement (« *Bring Your Own Key*, BYOK », parfois aussi « *Bring Your Own Encryption*, BYOE »). Toutefois, celle-ci doit être enregistrée et sauvegardée sur le cloud. Cependant, la conservation de la clé de chiffrement sur le cloud permet au CSP de décrypter et de donc de produire les données en vertu du *CLOUD Act*. Qu'il y soit autorisé ou non dépend en premier lieu des conditions d'utilisation et en second lieu de la pression exercée par les autorités américaines. Dans la troisième variante, le client sauvegarde la clé de chiffrement uniquement sur son propre disque dur. Pour cette variante, la protection est la

¹⁵⁵ « The terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data », *CLOUD Act*, § 2523(b)(3). Voir également DOJ, « Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the *CLOUD Act* », p. 6 ; ZAGARIS, « U.S. and UK Sign Cross-Border Data Access Agreement for Cross-Border Enforcement and Warn Facebook on Proposed Encryption », p. 360.

¹⁵⁶ Conformément au droit suisse, les CSPs ne peuvent être contraints de décrypter que les données qu'ils ont eux-mêmes cryptées (art. 26, al. 2, let. c LSCPT).

¹⁵⁷ RS 816.11

Rapport sur le US CLOUD Act (loi *Cloud*)

même que pour le cryptage côté client. Le CSP ne peut pas décrypter les données sans l'accord du client ou du propriétaire des données.

Dans ce contexte, ce qui suit apparaît comme une évidence: conformément au *CLOUD Act*, les CSPs ne sont pas tenus de décrypter les données dont ils disposent pour le compte de leurs utilisateurs ou clients¹⁵⁸. Nonobstant cette règle ou plutôt absence de règle, il faut être conscient du fait qu'un accès des autorités américaines à ces données ne peut pas être exclu, si un moyen technique ou un accord contractuel le permet.

7 Conclusion

Un des plus grands défis à relever dans le domaine de la coopération pénale internationale est la conservation et la production des preuves électroniques. Dans ce domaine, des approches nouvelles et innovantes sont nécessaires car la procédure actuelle rend très difficile la poursuite pénale au niveau international. Le présent rapport apporte des éclaircissements sur les différentes initiatives internationales visant à faciliter l'accès aux preuves électroniques: le Conseil de l'Europe élabore actuellement un deuxième protocole pour la Convention de Budapest, l'UE est en train d'adopter une législation *e-evidence* qui prescrit des règles européennes de conservation et de production des preuves électroniques et l'ONU prépare un instrument multilatéral pour lutter contre la cybercriminalité. Parallèlement à cela, on observe des évolutions dans les différents États. La plus importante initiative nationale est l'adoption du *CLOUD Act* par les USA. Pour les autorités de poursuite pénale américaines et les CSPs, cette loi fédérale américaine a une portée extraterritoriale. Elle permet aux autorités de poursuite pénale américaines d'accéder aux données des CSPs dont le siège est aux USA, que ces données soient enregistrées aux USA ou à l'étranger. En outre, la loi vise à « internationaliser » le système américain en donnant aux autorités américaines la possibilité de conclure un *executive agreement*, afin d'étendre le système et le domaine d'application du *CLOUD Act* aux autres États. Comme les plus grands CSPs ont leur siège aux USA, la collaboration avec cet État en matière de preuves électroniques a, notamment pour la Suisse, une importance particulière. C'est pourquoi, la question de la conclusion d'un éventuel *executive agreement* avec les USA fait débat. Le présent rapport traite cette question dans le contexte étendu du « Changement de paradigme dans le domaine de l'entraide pénale » et eu égard aux divers aspects juridiques qu'elle revêt. Il examine la compatibilité entre le *CLOUD Act* et le droit suisse, en particulier dans deux domaines: le droit de la protection des données et les principes de la coopération pénale internationale. L'OFJ est arrivé aux conclusions suivantes:

- Droit de la protection des données: les données concernées par le *CLOUD Act* sont des données personnelles au sens du droit de la protection des données. Dans ce contexte, il est particulièrement important qu'en cas de conclusion d'un *executive agreement*, les termes de cet accord soient compatibles avec le droit suisse de la protection des données. Le droit européen de la protection des données n'est certes pas directement applicable en Suisse, mais il est pris en compte de manière exhaustive dans le présent rapport. En effet, la Suisse est considérée par l'UE comme un État tiers avec un niveau adéquat de protection des données (décision d'adéquation), de sorte qu'elle peut échanger des données personnelles avec les États membres de l'UE et participer au libre flux des données avec l'UE. De ce fait, elle a un accès illimité au « *marché unique numérique* » de l'UE. Par conséquent, le droit européen de la protection des données a une grande influence sur la Suisse. De plus, le droit suisse de la protection des données vient d'être entièrement révisé. Le présent rapport analyse la compatibilité du *CLOUD Act* avec les versions actuelle et future du droit de la protection des données. Il ressort de cette analyse qu'une production de

¹⁵⁸ DASKAL, SWIRE, « The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards ».

Rapport sur le US CLOUD Act (loi *Cloud*)

données exigée au moyen d'une injonction de production adressée sur la base du *CLOUD Act* n'est compatible avec les droit suisse et européen de la protection des données que dans des cas exceptionnels et spécifiques.

- Droit de l'entraide judiciaire: le *CLOUD Act* permet à un CSP à l'étranger de transmettre des données électroniques à une autorité de poursuite pénale américaine, qui pourra ensuite utiliser les données et informations reçues dans le cadre d'une procédure pénale. Cette collaboration directe remplacerait, du moins en partie, la voie traditionnelle de l'entraide judiciaire. La conclusion d'un *executive agreement* entraînerait donc un *changement de paradigme* dans le domaine de la coopération pénale internationale: pour la première fois, une entité privée suisse participerait directement à une procédure pénale étrangère, sans qu'une procédure suisse ou du moins une autorisation soit en l'espèce nécessaire à cet effet. Cette nouvelle forme de collaboration aurait des effets sur les différents principes et garanties qui s'appliquent en vertu du droit de l'entraide pénale internationale. Elle impacterait en particulier les garanties constitutionnelles du droit d'être entendu et de la garantie de l'accès au juge, car la personne concernée par la production de données (propriétaire des données) n'aurait plus connaissance de leur divulgation et ne pourrait donc plus s'y opposer par voie de recours. L'OFJ ne pourrait plus jouer son rôle d'autorité de surveillance dans le cadre d'une procédure d'entraide judiciaire et donc garantir le respect des principes juridiques applicables en Suisse. La production dépendrait uniquement de la volonté de coopération du CSP. Ainsi, les droits d'une personne concernée par une requête d'entraide judiciaire seraient bafoués. Il en va de même de la possibilité pour l'État de contrôler la procédure et donc de garantir au final la souveraineté de la Suisse. Eu égard à la compatibilité avec les principes du droit de l'entraide judiciaire, le *CLOUD Act* soulève donc de grandes questions et semble difficilement compatible avec le droit suisse de rang supérieur.

8 Procédure à suivre

Le présent rapport est censé servir de *base à une discussion* avec les services partenaires à l'intérieur et à l'extérieur de l'administration fédérale, ainsi qu'avec les parties prenantes de l'économie privée, des associations professionnelles et des autres groupes de personnes intéressés. Sur la base des résultats de cette discussion, l'OFJ demandera en temps voulu au Secrétariat général du DFJP de lui indiquer la procédure à suivre en ce qui concerne le US *CLOUD Act* en l'espèce et les preuves électroniques en général.

9 Bibliographie

- BAERISWYL, B., « Vorbemerkungen zu Art. 4–11a » dans Baeriswyl, B. (Éditeur), *Datenschutzgesetz – Stämpfli Handkommentar*, Berne : Stämpfli 2015.
- BAERISWYL, B., « Art. 4 », dans Baeriswyl, B. (Éditeur), *Datenschutzgesetz – Stämpfli Handkommentar*, Berne : Stämpfli 2015.
- BAERISWYL, B., « Art. 10a », dans Baeriswyl, B. (Éditeur), *Datenschutzgesetz – Stämpfli Handkommentar*, Berne : Stämpfli 2015.
- BAERISWYL, B., BLONSKI, D., « Art. 6 », dans Baeriswyl, B. (Éditeur), *Datenschutzgesetz – Stämpfli Handkommentar*, Berne : Stämpfli 2015.
- BILGIC, S., « Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act », 32:1 2018 *Harvard Journal of Law and Technology*, p. 321.
- BISMUTH, R., « Le Cloud Act face au projet européen E-Evidence: confrontation ou coopération ? », dans *Revue critique de droit international privé*, 2019:3, p. 681.
- CHRISTAKIS, T., « 21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts) », *European Law Blog*, 17.10.2019, disponible sur : <https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/>.
- DASKAL, J., « Unpacking the CLOUD Act », 2018:4 *eu crim*, p. 220.
- DASKAL, J., « Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0 », 2018:71 *Stanford Law Review Online* p. 9, disponible sur : [Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0 | Stanford Law Review](#).
- DASKAL, J., SWIRE, P., « The UK-US CLOUD Act Agreement is Finally Here, Containing New Safeguards », *Just Security*, 08.10.2019, disponible sur : <https://www.justsecurity.org/66507/the-uk-us-cloud-act-agreement-is-finally-here-containing-new-safeguards/>.
- DASKAL, J., SWIRE, P., CHRISTAKIS, T., « The globalization of criminal evidence », 16.10.2018, disponible sur : <https://iapp.org/news/a/the-globalization-of-criminal-evidence/>.
- LUTZ T., EGLI L., « Braucht die Schweiz ein CLOUD Act executive agreement ? », *Schweizerische Juristen-Zeitung* SJZ 2021, p. 119.
- MAURER-LAMBROU, U., STEINER, A., « Art. 6 LPD », dans Maurer-Lambrou, U., Blechta, G.P. (Éditeur), *Basler Kommentar: Datenschutzgesetz – Öffentlichkeitsgesetz*, Bâle : Helbing Lichtenhahn 2014.
- MAURER-LAMBROU, U., STEINER, A., « Art. 4 LPD », dans Maurer-Lambrou, U., Blechta, G.P. (Éditeur), *Basler Kommentar: Datenschutzgesetz – Öffentlichkeitsgesetz*, Bâle : Helbing Lichtenhahn 2014.
- PLENACOSTE, F., DAOUD, E., « CLOUD Act: Des inquiétudes légitimes », 2018:12 *Droit de la propriété intellectuelle et du numérique*, p. 680.

Rapport sur le US CLOUD Act (loi Cloud)

RAMPINI, C., « ART. 13 LPD », dans Maurer-Lambrou, U., Blechta, G.P. (Éditeur), *Basler Kommentar: Datenschutzgesetz – Öffentlichkeitsgesetz*, Bâle : Helbing Lichtenhahn 2014.

ROSENTHAL, D., JÖHRI, Y., *Handkommentar zum Datenschutzgesetz*, Zurich : Schulthess 2008.

ROSENTHAL, D., « Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act », *Jusletter*, 10 août 2020.

TSILIKIS, D., « Auf der grenzüberschreitenden Suche nach E-Evidence im Strafverfahren: die Unionsrechtsperspektive im digitalen Zeitalter », dans Meier, J., Zurkinden, N., Staffler, L. (Éditeur), *Recht und Innovation – Innovation durch Recht, im Recht und als Herausforderung für das Recht*, Zurich : Dike 2020, p. 163.

ZAGARIS, B., « U.S. and UK Sign Cross-Border Data Access Agreement for Cross-Border Enforcement and Warn Facebook on Proposed Encryption », 35:10 2019 *International Enforcement Law Reporter*, p. 357.

ZERDICK, T., « Art. 48 – Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung » dans Ehmann, E., Selmayr, M. (Éditeur), *Datenschutz-Grundverordnung – Kommentar*, 2^e édition, Beck: Munich 2018.

ZIMMERMANN, R., *La coopération judiciaire internationale en matière pénale*, 5^e édition, Berne : Stämpfli 2019.

EDPB/CEPD, « Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence », 10 juillet 2019, disponible sur : https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf (EDPB/CEPD, Initial legal assessment).

US DOJ, « Promoting Public Safety, Privacy, and the Rule of Law around the World: The Purpose and Impact of the CLOUD Act », White Paper, 2019, disponible sur : <https://www.justice.gov/dag/page/file/1153436/download>.

Rapport sur le US CLOUD Act (loi *Cloud*)

10 Abréviations

al.	alinéa
art.	article
FF	Feuille fédérale
LF	Loi fédérale
LTEJUS	Loi fédérale relative au traité conclu avec les États-Unis d'Amérique sur l'entraide judiciaire en matière pénale
OFJ	Office fédéral de la justice
BSK	Commentaire bâlois
let.	lettre(s)
Convention de Budapest	Convention du Conseil de l'Europe sur la cybercriminalité (Convention sur la cybercriminalité)
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication
Cst.	Constitution fédérale de la Confédération suisse
CLOUD Act	<i>Clarifying Lawful Overseas Use of Data Act</i> (USA)
CSP	Communication Service Provider – fournisseur de services de communication
Convention 108+	Protocole d'amendement à la Convention du Conseil de l'Europe pour la protection des données
Service SCPT	Service chargé de la surveillance de la correspondance par poste et télécommunication
DOJ	Département américain de la justice
LPD	Loi fédérale sur la protection des données
RGPD	Règlement général de l'UE sur la protection des données
PFPDT	Préposé fédéral à la protection des données et à la transparence
EDPB	Comité européen de la protection des données
CEPD	Contrôleur européen de la protection de données
Directive décision d'enquête européenne	Directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale
Preuve électronique	Mesures de l'UE pour améliorer l'accès transfrontière aux preuves électroniques
CourEDH	Cour européenne des droits de l'homme
CEDH	Convention européenne des droits de l'homme
EPOC	Injonction européenne de production
EPOC-PR	Injonction européenne de conservation
consid.	considérant
EUeR	Convention européenne d'entraide judiciaire en matière pénale
CJUE	Cour de justice de l'Union européenne
FST	Fournisseurs de services de télécommunication
FINMA	Autorité fédérale de surveillance des marchés financiers
LTC	Loi sur les télécommunications
SG-DFJP	Secrétariat général du Département fédéral de justice et police
EIMP	Loi fédérale sur l'entraide internationale en matière pénale (loi sur l'entraide pénale internationale)
OEIMP	Ordonnance sur l'entraide internationale en matière pénale
nLPD	Révision totale de la loi sur la protection des données du 25.9.2020
Org DFJP	Ordonnance sur l'organisation du Département fédéral de justice et police
GEQ	Gouvernement étranger qualifié (État ayant signé un <i>executive agreement</i> avec les USA)
TEJUS	Traité entre la Suisse et les États-Unis sur l'entraide judiciaire en matière pénale
SCA	<i>Stored Communications Act</i> (USA)
LPDS	Loi fédérale sur la protection des données dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal
STCE	Série des traités du Conseil de l'Europe

Rapport sur le US CLOUD Act (loi *Cloud*)

CS	Commentaire Stämpfli
RS	Recueil systématique du droit fédéral
CPJI	Cour permanente de justice internationale (dissolution en 1946)
CP	Code pénal suisse
CPP	Code de procédure pénale suisse
T-CY	Comité du Conseil de l'Europe de la Convention sur la cybercriminalité
GBR	Royaume-Uni
OLPD	Ordonnance relative à la loi fédérale sur la protection des données
PA	Loi fédérale sur la procédure administrative
WVK	Convention de Vienne sur le droit des traités
ch.	chiffre