Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la justice OFJ

Synthèse des résultats de la procédure de consultation

relative au rapport et à l'avant-projet

concernant

la modification de la loi fédérale

du 6 octobre 2000

sur la surveillance de la correspondance par poste et télécommunication (LSCPT)

Berne, mai 2011

Table des matières

Liste des participants à la procédure de consultation avec leur sigle

CANTONS

Regierungsrat Kt. Zürich	ZH
Regierungsrat Kt. Bern	BE
Regierungsrat Kt. Luzern	LU
Regierungsrat Kt. Uri	UR
Regierungsrat Kt. Schwyz	SZ
Regierungsrat Kt. Obwalden	OW
Regierungsrat Kt. Nidwalden	NW
Regierungsrat Kt. Glarus	GL
Regierungsrat Kt. Zug	ZG
Conseil d'Etat du canton de Fribourg	FR
Regierungsrat Kt. Solothurn	SO
Regierungsrat Kt. Basel-Stadt	BS
Regierungsrat Kt. Basel-Landschaft	BL
Regierungsrat Kt. Schaffhausen	SH
Regierungsrat Kt. Appenzell Ausserrhoden	AR
Standeskommission Kt. Appenzell Innerrhoden	AI
Regierungsrat Kt. St. Gallen	SG
Regierungsrat Kt. Graubünden	GR
Regierungsrat Kt. Aargau	AG
Regierungsrat Kt. Thurgau	TG
Consiglio di Stato del Cantone del Ticino	TI
Conseil d'Etat du canton de Vaud	VD
Conseil d'Etat du canton de Valais	VS
Conseil d'Etat du canton de Neuchâtel	NE
Conseil d'Etat du canton de Genève	GE
Gouvernement du canton du Jura	JU

PARTIS POLITIQUES

CSP Christlich-soziale Partei
PCS Parti chrétien-social
PCS Partito cristiano sociale
PCS Partida cristian-sociala

CVP Christlichdemokratische Volkspartei der Schweiz
PDC Parti démocrate-chrétien suisse
PPD Partito popolare democratico svizzero
PCD Partida cristiandemocrata svizra

FDP**.** Die Liberalen
PLR. Les Libéraux-Radicaux
PLR. I Liberali
PLD. Ils Liberals

GPS Grüne Partei der Schweiz
PES Parti écologiste suisse
I Verdi Partito ecologista svizzero
La Verda Partida ecologica svizra

PPS : Piratenpartei Schweiz
PPS : Parti Pirate Suisse

SP Schweiz Sozialdemokratische Partei der Schweiz
PS Parti socialiste suisse
PS Partito socialista svizzero
PS Partida socialdemocrata da la Svizra

SVP Schweizerische Volkspartei
UDC Union Démocratique du Centre
UDC Unione Democratica di Centro
PPS Partida Populara Svizra

ORGANISATIONS FAITIERES NATIONALES DES COMMUNES, DES VILLES ET DES REGIONS DE MONTAGNE

SSV Schweizerischer Städteverband
UVS Union des villes suisses
Unione delle città svizzere

ORGANISATIONS FAITIERES NATIONALES DE L'ECONOMIE

economiesuisse economiesuisse
Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss business federation

SGB Schweiz. Gewerkschaftsbund
USS Union syndicale suisse
USS Unione sindacale svizzera

SAG Schweizerischer Arbeitgeberverband
UPS Union patronale suisse
Unione svizzera degli imprenditori

SBV Schweizerischer Bauernverband
USP Union suisse des paysans
USC Unione svizzera dei contadini

AUTRES ORGANISATIONS, INSTITUTIONS ET PARTICULIERS

Cablecom GmbH	Cablecom
Centre Patronal	CP
Chaos Computer Club Zürich	CCC
Cognizant Technology Solutions S.A	COG
Colt Telecom Services AG	Colt

DJS Demokratische Juristinnen und Juristen der Schweiz
JDS Juristes Démocrates de Suisse
GDS Giuristi e Giuriste Democratici Svizzeri

Die Schweizerische Post
La Poste Suisse

ESBK Eidgenössische Spielbankenkommission
CFMJ Commission fédérale des maisons de jeu
CFCG Commissione federale delle case da gioco

„ePower für die Schweiz“ Parlamentariergruppe	ePower

ETH Eidgenössische Technische Hochschule Zürich
EPFZ Ecole polytechnique fédérale de Zurich

Finecom Telecommunications AG	Finecom

grundrechte.ch (gr.ch)
droitsfondamentaux.ch
dirittifondamentali.ch

Hauser Ralf	HR
Hewlett-Packard (Schweiz) GmbH	hp
ICTSwitzerland Information and Communication Technology	ICT

ifpi Schweiz (Dachverband der Ton- und Tonbildträgerhersteller)	ifpi
Information Security Society Switzerland	ISSS
INT Informatik AG	INT
Komitee für eine freie Gesellschaft	KFG
KKJPD Konferenz der kantonalen Justiz- und Polizeidirektoren **CCDJP Conférence des directrices et directeurs des départements cantonaux de justice et police** CDDGP Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia	
KKPKS Konferenz der kantonalen Polizeikommandanten der Schweiz **CCPCS Conférence des commandants des polices cantonales de suisse** CCPCS Conferenza dei comandanti delle polizie cantonali della svizzera	
KSBS Konferenz der Strafverfolgungsbehörden der Schweiz **CAPS Conférence des autorités de poursuite pénale de Suisse (CAPS)** CAIS Conferenza della autorità inquirenti svizzere (CAIS)	
Konsumentenforum kf	kf
Métille Sylvain	MS
Orange Communications SA	Orange
privatim - Die schweizerischen Datenschutzbeauftragten **privatim - Les commissaires suisses à la protection des données** privatim - Gli incaricati svizzeri della protezione dei dati	
Rosenthal David	RD
SIK Schweizerische Informatikkonferenz **CSI Conférence suisse sur l'informatique** Conferenza svizzera sull'informatica	
SKG Schweizerische Kriminalistische Gesellschaft **SSDP Société Suisse de droit pénal** SSDP Società svizzera di diritto penale	
Schweizerische Vereinigung zur Bekämpfung der Piraterie **Association suisse pour la lutte contre le piratage**	safe
SAV Schweizerischer Anwaltsverband **FSA Fédération suisse des avocats** FSA Federazione svizzera degli avvocati	
Schweizerischer Verband der Telekommunikation **Association Suisse des Télécommunications**	asut

SPI Schweizerisches Polizei-Institut **ISP Institut suisse de police** ISP Istituto svizzero di polizia)	
Sitrox AG	Sitrox
Stiftung für Konsumentenschutz **Fondation pour la protection des consommateurs**	SKS
Sunrise Communications AG	Sunrise
SWICO (Der Wirtschaftsverband für die Digitale Schweiz)	SWICO
SIMSA swiss internet industry association	SIMSA
Swiss Internet User Group	SIUG
SWISS POLICE ICT (Responsable du Congrès informatique des polices de Suisse SPIK)	SPICT
Swisscable (Association de branche des câblo-opérateurs suisses)	Swisscable
Swisscom (Schweiz) AG	Swisscom
SWITCH Serving Swiss Universities	switch
Switchplus AG	switchplus
Entreprises regroupées sous le vocable IT (19) **:**	IT(19)

United Security Providers AG
Fargate AG
Futurecom Interactive AG
OneConsult GmbH
Stories AG
Neidhart + Schön Group AG
Viollier Consulting AG
midix.com ag
Open systems ag
Namics AG
InVisible GmbH
Köpfli & Partner AG
Dinotronic AG
terreActive
von salis engineering GmbH
Dr. Hartwig Thomas
Icontel AG
ISPIN AG
WIRZ Grupppe

Universität St. Gallen **Université de St-Gall**	UNISG
Universität Zürich **Université de Zurich**	UNIZH
VSPB Verband Schweizerischer Polizei-Beamter **FSFP Fédération suisse des fonctionnaires de police** FSFP Federazione svizzera dei funzionari di polizia (FSFP)	
Verein Swiss Privacy Foundation **Association suisse pour la sphère privée** (Swiss Privacy Foundation)	VSPF
Verizon Switzerland AG	Verizon
3D4X Internetagentur & Softwareentwicklung	3D4X

I. Introduction

Le 19 mai 2010[1], le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP) d'ouvrir une procédure de consultation concernant l'avant-projet[2] (AP) de modification de la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT)[3] et le rapport explicatif s'y rapportant[4]. Il est ici question d'une révision totale de la LSCPT ayant principalement pour but d'adapter la loi aux évolutions techniques de ces dernières années, en particulier dans le domaine d'Internet.

Dans un courrier daté du 19 mai 2010, le DFJP a invité les cantons, les partis représentés à l'Assemblée fédérale ainsi que les organisations et associations intéressées à donner leur avis sur l'AP jusqu'au 18 août 2010.

Les avis exprimés (106 au total) représentent quelque 700 pages. Sur les 93 destinataires priés de se prononcer, il y a eu 55 réponses, dont quatre refus explicites de prendre position sur le fond de l'AP. 51 participants ont donc pris part spontanément à la procédure de consultation.

Ont pris position :

26 cantons

6 partis politiques

74 milieux intéressés.

---

1 http://www.bj.admin.ch/content/bj/fr/home/dokumentation/medieninformationen/2010/ref_2010-05-19.html

2 http://www.bj.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/entw-f.pdf

3 RS 780.1

4 http://www.bj.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/vn-ber-f.pdf

II. Vue d'ensemble des résultats

1. Appréciation générale

Tous les participants ont reconnu ou, du moins, n'ont pas remis en cause, la nécessité d'adapter la LSCPT aux évolutions techniques de ces dernières années, en particulier dans le domaine d'Internet. Cependant, nombre de réserves, en partie structurelles et générales, ont été émises en ce qui concerne les diverses dispositions proposées. Un remaniement complet a même parfois été requis. Plusieurs participants[5] critiquent, en outre, la complexité du langage employé dans l'AP. Ci-après, sont tout d'abord mentionnés les participants qui ont approuvé l'AP sans restriction (ch. 2), puis sont exposées les principales réserves (ch. 3). Enfin, dans la partie III, sont récapitulées les remarques des participants sur les différentes dispositions.

2. Approbation sans réserve

Trois cantons (UR, OW, GE) et la Poste Suisse (en ce qui concerne la surveillance de la correspondance par poste) approuvent l'AP sans réserve.

3. Principales réserves

Champ d'application à raison des personnes (art. 2 AP)

Quelques participants[6] déplorent d'une manière générale que le libellé de l'art. 2 AP ne fasse pas ressortir clairement à qui s'adresse concrètement la LSCPT. Nombreux[7] sont ceux qui s'opposent à l'extension du champ d'application à raison des personnes prévue par l'art. 2, al. 1, let. b, AP et qui demandent une limitation de celui-ci, une suppression de la disposition ou, du moins, une reformulation. S'agissant de l'art. 2, al. 2, AP, certains participants souhaitent qu'on précise clairement à quelles personnes il s'adresse concrètement[8] et qu'on indique quels devoirs incombent à ces personnes[9] en relation avec l'art. 26 AP. PES, USS et INT attirent, en outre, l'attention sur le fait que l'extension du champ d'application peut menacer l'existence de certaines entreprises, en particulier les petites. RD trouve contraire au système que le champ d'application de la LSCPT soit étendu à des personnes n'étant pas soumises au secret des télécommunications.

Système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication (art. 6 à 13 AP)

De nombreux participants[10] s'opposent à une conservation centralisée et durable des données au sein du service de surveillance (ci-après « service ») et, sur le principe, se déclarent plutôt favorables au maintien de l'ancien système (enregistrement des données, copie sur supports de données, transmission aux autorités chargées de l'enquête, effacement des

---

5 BE, SZ, NW, SH, LU, SH, PDC, CAPS, SSDP.
6 FR, VD, PDC, ISSS, CP, RD.
7 PLR, PPS, SIUG, Swiss Privacy Foundation, switch, switchplus, RD, SWICO, hp, COG, ISSS, JDS, droitsfondamentaux.ch, SKS, PES, USS, KFG, INT, SIK, asut, Finecom, Orange, Swisscom, Colt, Verizon.
8 LU, EPFZ, UNISG, asut, Swisscom, Finecom, Orange, Colt, Sunrise, Verizon, Swisscable, switch.
9 LU, BL, AR, PS, privatim.
10 SO, BE, NW, BL, LU, SZ, SO, SG, SH, SSDP, CAPS.

données au sein du service). Quelques participants[11] aimeraient qu'on inscrive dans la loi le fait que l'envoi postal de supports de données et de documents (système actuel) peut encore s'avérer nécessaire dans certaines circonstances particulières (p. ex., dans le cadre de l'entraide judiciaire internationale). D'autres[12] souhaitent, eu égard à la quantité considérable de données recueillies dans le domaine de la surveillance d'Internet, que celles-ci soient conservées de façon centralisée et durable et puissent être consultées moyennant un droit d'accès au système, mais que les surveillances téléphoniques continuent d'être enregistrées et les enregistrements envoyés sur des supports de données. Plusieurs participants[13] considèrent que le nouveau système porte atteinte aux droits des parties, ces dernières devant avoir accès aux originaux conformément au code de procédure pénale du 5 octobre 2007 (CPP)[14]. L'idée que les parties puissent consulter les données est rejetée pour des raisons de sécurité. Un grand nombre de participants[15] estime que la règle prévue par l'art. 10 AP en ce qui concerne le droit de consulter le dossier et le droit d'accès aux données est inutile car le CPP contient suffisamment de dispositions visant à protéger les données personnelles. Selon plusieurs participants[16], le fait que les délais de conservation des données soient calqués sur les délais de prescription (art. 11 AP) est trop compliqué et coûteux. C'est la raison pour laquelle ils déclarent vouloir conserver l'ancien système. Pour eux, les délais de conservation des données doivent être fixés uniquement d'après le CPP.

Obligation manquante du service de vérifier la légalité des ordres de surveillance et voies de droit

Un grand nombre de participants[17] exige que le service soit soumis à l'obligation de vérifier la légalité des surveillances ordonnées (v. infra, partie III, ch. 3.2.1, remarques concernant l'art. 15, let. a, AP et partie III, ch. 3.3.1, remarques concernant l'art. 16, let. a, AP) et que soit donc prévue à l'art. 34 AP (Voies de droit) la possibilité pour les personnes tenues d'exécuter une surveillance de faire examiner par un tribunal la légalité de l'ordre de surveillance qui leur a été donné. Quelques participants[18] considèrent que l'absence d'une telle obligation est en contradiction avec l'art. 33 AP, qui statue que le service doit veiller à ce que la législation relative à la surveillance de la correspondance par poste et télécommunication soit respectée.

Obligations lors de l'exécution de surveillances (art. 21 AP)

Pour un groupe important de participants[19], les obligations concrètes qui incombent aux personnes tenues d'exécuter une surveillance ne sont pas réglées de manière suffisamment claire. Par souci d'assurer la sécurité du droit, ils demandent donc, en proposant parfois des formulations concrètes, que soit prévu un cahier des charges clair.

---

11 ZH, LU, AG, GL, GR, TG, VS, JU, CCDJP, CCPCS, CCC.
12 LU, SZ, SO, SG, SH, CAPS.
13 BE, NW, BS, BL, SSDP, FSA, MS.
14 RO 2010 1881; en vigueur depuis le 1.1.2011.
15 LU, NW, BL, SG, GL, TG, VS, JU, CCDJP, CAPS, SSDP.
16 BE, SZ, NW, BL, SH, SG, AG, VD, CAPS.
17 ZG, BE, BL, AR, PLR, PS, Swisscable, SWICO, UVS, Cablecom, asut, Orange, Swisscom, Colt, Sunrise, Verizon, CAPS, privatim, economiesuisse, SIUG, hp, COG, ISSS, Swiss Privacy Foundation, PES, IT(19).
18 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, SWICO, hp, COG.
19 PDC, PLR, UDC, PES, SKS, economiesuisse, ICT, ePower, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, SIUG, SPICT.

Identification des utilisateurs qui accèdent à Internet (art. 22 AP)

De nombreux participants[20] demandent la suppression ou l'adaptation de cette disposition. Ils considèrent qu'il serait disproportionné, voire irréalisable, d'obliger tous les utilisateurs qui accèdent à Internet à s'identifier. Ils relèvent en outre qu'il existe de nombreuses possibilités d'éluder cette obligation.

Allongement du délai de conservation des données à douze mois (art. 23 AP)

Un grand nombre de participants[21] s'oppose à cette disposition – certains renvoyant aux critères fixés par la Cour constitutionnelle allemande[22] en ce qui concerne la conservation préventive de données – ou demande qu'elle soit modifiée. Ils sont quelques-uns[23] à souligner que les autorités conservent systématiquement à titre préventif des données sur des personnes au-dessus de tout soupçon.

Suppression de l'indemnisation des personnes tenues d'exécuter des surveillances (art. 30, al. 1, AP)

De nombreux participants[24] sont contre la suppression, prévue par l'AP, de l'indemnisation des personnes tenues d'exécuter des surveillances. La plupart d'entre eux[25] soulignent que la poursuite pénale est une tâche qui incombe à l'Etat et qu'elle doit donc être prise en charge par la collectivité. Quelques participants[26] attirent l'attention sur la nécessité de se doter d'une infrastructure coûteuse pour satisfaire aux nouvelles exigences de la loi. Certains[27] souhaitent une réglementation plus nuancée.

Interception et décryptage de données (art. 270bis CPP) ; introduction de programmes informatiques dans des systèmes informatiques de tiers

Dix participants[28] se déclarent opposés à l'introduction de programmes informatiques dans des systèmes informatiques de tiers (« Government Software », souvent aussi appelés « chevaux de Troie ») ; ils sont plus nombreux encore[29] à émettre d'importantes réserves à ce sujet. Ils pointent en particulier du doigt la grave atteinte à la vie privée des personnes concernées que constituerait la possibilité d'accéder à toutes les données contenues dans un système informatique. Certains déplorent par ailleurs le fait que nulle part il n'est fait référence à l'arrêt de principe relatif aux « perquisitions en ligne » rendu par la Cour constitution-

---

20 VD, PES, UDC, PLR, ISSS, UVS, privatim, JDS, droitsfondamentaux.ch, RD, IT(19), Cablecom, switch und switchplus, CP, FSA, KFG, PPS, EPFZ, UNISG, UNIZH.

21 BL, PES, PS, SKS, USS, JDS, droitsfondamentaux.ch, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SIUG, ISSS, SWICO, hp, privatim, COG, 3D4X, PPS.

22 V. note de bas de page 120 et les remarques dans la partie III, ch. 5.4.

23 JDS, droitsfondamentaux.ch, PES, SKS.

24 PS, PDC, PLR, UDC, PES, PPS, JDS, droitsfondamentaux.ch, RD, ISSS, MS, SIUG, SIMSA, INT, asut, Finecom, Orange, Swisscom, Sunrise, Colt, Verizon, Cablecom, FSA, SKS, Swisscable, CP, CCC, Sitrox, economiesuisse, IT(19), SWICO, hp, COG.

25 PDC, PLR, UDC, PES, asut, Finecom, Orange, Swisscom, Sunrise, Verizon, Cablecom, FSA, SKS Swisscable, SIUG, CP, CCC, Sitrox, PPS.

26 PS, Colt, SIUG, SIMSA, INT, ISSS, PPS, PES.

27 Le PDC veut que les coûts liés à l'augmentation de la capacité des systèmes soient indemnisés alors que le PS souhaite une différenciation en fonction de la taille de l'entreprise ou de la capacité économique.

28 PES, JDS, droitsfondamentaux.ch, Cablecom, CCC, SKS, SIUG, KFG, PPS, ISSS.

29 ZH, BL, AR, LU, PS, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SIUG, privatim, economiesuisse, Swisscable.

nelle allemande[30]. Nombre de participants[31] expriment les inquiétudes en matière de sécurité que leur inspirent non seulement le programme informatique lui-même ou son utilisation abusive par un criminel mais encore le système informatique ou le réseau dans lequel le programme informatique doit être introduit. BS, FR, PS et privatim souhaitent que la liste des infractions pour lesquelles l'art. 269, al. 2, let. a, CPP autorise la Confédération à recourir aux « chevaux de Troie » soit réduite.

III. Remarques des participants sur les différentes dispositions de l'AP

1. Dispositions générales

1.1. Art. 1 Champ d'application à raison de la matière

[1] La présente loi s'applique à la surveillance de la correspondance par poste et télécommunication, y compris par Internet, qui est ordonnée et mise en œuvre :

a. dans le cadre d'une procédure pénale;

b. lors de l'exécution d'une demande d'entraide;

c. dans le cadre de la recherche de personnes disparues;

d. dans le cadre de la recherche de personnes condamnées à une peine privative de liberté ou qui font l'objet d'une mesure entraînant une privation de liberté.

[2] Les renseignements sur les services de paiement soumis à la loi du 30 avril 1997 sur la poste sont régis par les art. 284 et 285 du code de procédure pénale du 5 octobre 2007 (CPP).

1.1.1 Art. 1, al. 1

Quelques participants[32] considèrent que les concepts de « correspondance par poste et télécommunication » et de « correspondance par Internet » utilisés à l'al. 1 sont trop imprécis. Dire que la « correspondance par Internet » fait partie de la « correspondance par poste et télécommunication » démontre, selon PPS, qu'on n'a pas compris le fonctionnement de ce moyen de communication sui generis qu'est Internet, celui-ci n'étant ni un téléphone ni un fax amélioré. Pour UNISG, switch et switchplus, on ne sait notamment pas très bien si, p. ex., l'utilisation d'autres services basés sur les protocoles TCP[33]/IP[34] comme HTTP[35], FTP[36] et Telnet[37] doit être considérée comme de la correspondance par Internet au sens où l'entend la loi. Pour UNIZH, la même incertitude règne en ce qui concerne des services comme Skype[38], PPTP[39] et Teredo[40]. asut pense que seule la communication individuelle devrait faire l'objet de mesures de surveillance, autrement dit que seuls certains raccordements devraient être surveillés. FSFP estime, pour sa part, que les concepts susmentionnés sont trop restrictifs eu égard aux progrès technologiques qui vont encore être réalisés et qu'une formulation plus simple et plus générale mais aussi et surtout plus flexible devrait être adoptée.

A propos de la nouvelle possibilité prévue par l'AP de recourir à la surveillance de la corres-

---

30 BVerfG, 1 BvR 370/07 du 27.2.2008, para. 1 à 333; voir aussi III, ch. 11.1.2.
31 PES, JDS, droitsfondamentaux.ch, SKS, KFG, PPS, SIUG.
32 VD, UNIZH, PPS, UNISG, switch, switchplus, EPFZ.
33 Transmission Control Protocol.
34 Internet Protocol.
35 Hypertext Transfer Protocol.
36 File Transfer Protocol.
37 Telecommunication Network.
38 Logiciel gratuit de VoIP (Voice over IP).
39 Point-to-Point Tunneling Protocol.
40 Teredo est un protocole de communication qui permet l'échange de données sur Internet.

pondance par poste et télécommunication pour rechercher des personnes condamnées, voir les remarques concernant l'art. 28 AP dans la partie III, ch. 6.2.

1.1.2 Art. 1, al. 2

Pas de remarques.

1.2. Art. 2 Champ d'application à raison des personnes

> *[1] Les surveillances fondées sur la présente loi sont exécutées par:*
>
> *a. les fournisseurs de services postaux et de télécommunication, y compris les fournisseurs d'accès à Internet, qui exercent leur activité à titre professionnel;*
>
> *b. les personnes qui, à titre professionnel, administrent des données de communication pour les personnes mentionnées à la let. a, transfèrent à des tiers des données de communication ou mettent à disposition l'infrastructure nécessaire à cet effet.*
>
> *[2] Les exploitants de réseaux de télécommunication internes et de centraux domestiques ainsi que les personnes mentionnées à l'al. 1 qui n'exercent pas leur activité dans le domaine de la correspondance par télécommunication à titre professionnel sont tenus de tolérer une surveillance au sens de la présente loi.*

Plusieurs participants[41] demandent en termes généraux que l'art. 2 soit précisé car ils estiment qu'on ne peut déterminer clairement à qui il s'adresse concrètement.

NE, EPFZ et UNISG proposent de remplacer l'expression « qui exercent leur activité à titre professionnel » par « qui exercent une activité commerciale ». D'autres participants[42] souhaitent qu'elle soit remplacée par « qui exercent une activité commerciale à but lucratif ».

1.2.1 Art. 2, al. 1, let. a

Quelques participants[43] déplorent que le concept de « fournisseur d'accès à Internet » ne soit pas défini dans la loi. switch propose que soient considérés comme « fournisseurs d'accès à Internet » ceux qui proposent des services de messagerie électronique et de téléphonie par IP.

1.2.2 Art. 2, al. 1, let. b

Un grand nombre de participants[44] estime que l'extension du champ d'application prévue par l'AP est absolument nécessaire et urgente. Kf apprécie le fait que soit déterminé avec une plus grande précision qui est soumis à la nouvelle LSCPT.

Nombreux[45] sont également ceux qui, au contraire, s'opposent à une extension du champ d'application à raison des personnes et qui demandent une limitation de ce dernier, la suppression ou, du moins, une reformulation de la let. b. Selon quelques participants[46], l'extension du champ d'application implique que tous les fournisseurs de services, de contenus ou de prestations techniques nécessaires à l'utilisation ou à l'exploitation de contenus et

---

41 FR, VD, PDC, ISSS, CP, RD.
42 switch, asut, Finecom, Swisscom, Colt, Sunrise, Verizon.
43 SIUG, switch, switchplus, HR, EPFZ, UNISG.
44 ZH, ZG, LU, SZ, NW, AR, SO, SH, SG, GR, AG, TG, TI, VS, NE, GE, JU, PLR, ICT, ePower, SPICT, CCDJP, CCPCS, CAPS.
45 PLR, SIUG, Swiss Privacy Foundation, switch, switchplus, RD, PPS, SWICO, hp, COG, ISSS, JDS, droitsfondamentaux.ch, SKS, PES, USS, KFG, INT, SIK, asut, Finecom, Orange, Swisscom, Colt, Verizon.
46 SIUG, Swiss Privacy Foundation, switch, switchplus, RD, PPS.

de services sur Internet, autrement dit, comme le relèvent RD et PPS, toutes les entreprises qui, d'une manière ou d'une autre, ont affaire à des données de communication à titre professionnel, sont désormais soumis à la LSCPT. Ainsi, les entreprises et les personnes de toute une branche économique sont tenues d'exécuter des surveillances actives, de se doter des équipements nécessaires à cet effet et de mettre à disposition du personnel, et ce à leurs frais. Une telle extension est disproportionnée et donc inacceptable. Certains demandent que le champ d'application reste limité aux fournisseurs d'accès à Internet professionnels et ne s'étende pas aux fournisseurs d'hébergement et de contenu.

Par ailleurs, plusieurs participants[47] veulent limiter le champ d'application de la LSCPT aux entreprises, autrement dit aux personnes morales qui fournissent des services de télécommunication ou qui administrent, à titre professionnel[48] ou dans le cadre d'une activité commerciale à but lucratif[49], des données de communication pour des fournisseurs de services de télécommunication.

Selon SIMSA, le critère déterminant lors de la désignation des personnes tenues d'exécuter des surveillances doit être le fait qu'elles proposent des moyens de communication individuelle. Selon JDS et droitsfondamentaux.ch, la volonté de soumettre toutes les formes de communication possibles à une surveillance transparaît au travers du fait que le champ d'application à raison des personnes de la LSCPT est élargi.

SKS, PES, USS et KFG trouvent effarant qu'on ne parle pas des conséquences qu'entraîne l'extension du champ d'application pour les personnes censées être dorénavant soumises à la LSCPT. Selon PES et USS, les coûts d'investissement nécessaires à l'exécution des surveillances sont problématiques pour les petits fournisseurs locaux, pour ne pas dire qu'ils pourraient même menacer leur existence. Petit fournisseur d'hébergement sur Internet directement concerné par l'extension du champ d'application de la LSCPT, INT pense que la révision, eu égard aux coûts qu'elle engendrera, sera extrêmement nuisible à l'économie car les petites entreprises en particulier ne seront pour ainsi dire plus en mesure d'exploiter une infrastructure de communication en conformité avec la loi. Par ailleurs, à l'ère d'Internet, n'importe quel utilisateur a à sa disposition des moyens fiables et gratuits pour crypter et anonymiser ses données (p. ex., Tor ou Freenet), si bien que toute surveillance d'Internet est vaine. La révision est, par conséquent, inutile et ne prend pas en considération les intérêts des PME.

RD relève, en outre, qu'il n'est pas possible, ne serait-ce que pour des raisons pratiques, d'étendre le champ d'application de la LSCPT à des exploitants de plates-formes de messagerie électronique comme GMX, Hotmail ou Gmail, dans la mesure où ces derniers sont installés à l'étranger, c'est-à-dire là où la LSCPT n'est pas applicable. De plus, l'extension prévue ne résout pas le problème lié au fait que l'utilisateur final crypte ses communications ou ses données (problème de Skype) et qu'il ne confie pas sa clé de cryptage à son fournisseur d'accès (qu'il soit considéré ou non comme un fournisseur de services de télécommunication au sens où l'entend la loi). Il ne faut pas non plus oublier les raisons pour lesquelles la LSCPT a été créée. L'une d'entre elles est que les fournisseurs de services de télécommunication sont soumis au secret des télécommunications et qu'il fallait donc régler dans une loi la question de savoir quand et comment ils devaient livrer les informations couvertes par ce secret. Cela signifie cependant aussi qu'il est contraire au système d'étendre le champ d'application de la LSCPT à des personnes qui ne sont pas soumises au secret des télé-

---

47 asut, Finecom, Orange, Swisscom, Colt, Verizon, SWICO, hp, COG, ISSS.
48 Orange, Cablecom.
49 asut, Finecom, Orange, Swisscom, Colt, Verizon.

communications. Les autres fournisseurs qui doivent entrer dans le champ d'application de la LSCPT ne sont soumis qu'exceptionnellement au secret des télécommunications. Dans la mesure où on peut avoir accès à leurs documents par les voies ordinaires prévues par la procédure pénale, rien ne justifie qu'on les soumette à la LSCPT. Le faire pourrait compliquer le travail des autorités de poursuite pénale car on pourrait faire valoir que la réglementation prévue par une loi spéciale déroge à toutes les autres règles générales sur la remise de documents, la transmission de renseignements et la confiscation. L'extension prévue du champ d'application de la LSCPT s'avère, en outre, problématique puisque les obligations ont été conçues « sur mesure » pour les fournisseurs de services de télécommunication et qu'on ne sait pas très bien comment les personnes qui seront dorénavant soumises à la LSCPT pourront les satisfaire. On pense, p. ex., aux administrateurs de sites Web disposant d'une fonctionnalité permettant aux personnes de se faire parvenir entre elles des communications. Non seulement ils administrent un serveur de messagerie pour des tiers ou le raccordent au serveur d'un fournisseur de services de télécommunication, mais aussi ils acheminent, à chaque opération de transmission, les e-mails de tiers vers le serveur de messagerie des destinataires. On peut aisément faire valoir qu'il s'agit d'entreprises qui transmettent à titre professionnel des données de communication à des tiers ou qui mettent à disposition l'infrastructure nécessaire à cet effet. Par ailleurs, d'innombrables fournisseurs d'hébergement sur Internet seraient inclus dans le champ d'application de la LSCPT, y compris ceux qui proposent des plates-formes de commerce en ligne comme eBay ou Ricardo et toutes les entreprises qui autorisent des tiers à laisser des commentaires sur leur site Web (p. ex., un livre d'or ou un blog). Car, en fin de compte, ces derniers transmettent, eux aussi, des données de communication (p. ex., le contenu d'une petite annonce) à des tiers (les visiteurs) ou mettent à disposition l'infrastructure nécessaire à cet effet. Le rapport explicatif dit clairement à la page 17 que les fournisseurs d'hébergement (Service-Provider ; Hosting-Provider) sur Internet doivent être inclus dans le champ d'application de la LSCPT. Tous les médias électroniques qui publient des courriers de lecteurs ou des petites annonces en ligne sont aujourd'hui également considérés comme tels et doivent donc, à l'évidence, entrer dans le champ d'application de la LSCPT. Toutes ces entreprises doivent par conséquent mettre en place, à leurs frais, des infrastructures importantes pour pouvoir remplir les obligations prévues par la loi. Il est sans aucun doute tentant pour les autorités de poursuite pénale de pouvoir, à tout moment, avoir un œil sur tout ce qui se passe sur Internet. Cela ne peut et ne doit pas pour autant être le but de la LSCPT qui vise uniquement la surveillance de la correspondance par télécommunication et non de toutes les branches du monde « numérique ». RD ne connaît aucun Etat occidental qui surveille autant Internet que ne le prévoit en fin de compte l'AP. La formulation de l'art. 2, al. 1, let. b, AP laisse à penser que même les exploitants de réseaux de télécommunication internes et de centraux domestiques, qui sont mentionnés à part à l'al. 2, sont désormais soumis à la LSCPT dans la mesure où ils mettent à disposition l'infrastructure nécessaire au transfert de données de communication à des tiers. Même si l'on peut objecter à cela que ce n'est pas la correspondance de l'entreprise elle-même qui est visée, de nombreuses entreprises pourraient malgré tout être concernées, en particulier celles qui autorisent leurs collaborateurs à avoir des conversations téléphoniques privées et à envoyer des e-mails ou celles qui font office de centres de services télécom ou informatiques dans des groupes d'entreprises et qui, de par leur fonction, sont amenées à fournir des services de télécommunication à d'autres sociétés du groupe. Là encore, les conséquences de l'extension du champ d'application à raison des personnes prévue par l'AP sont disproportionnées. Les entreprises qui fournissent des services dans le domaine de la sécurité des réseaux (p. ex. Managed Security Services) en surveillant et en administrant, p. ex., des réseaux d'entreprises, peuvent entrer dans le champ d'application de la LSCPT. On peut, en effet, considérer qu'en fournissant un pare-feu, ils mettent à disposition à titre professionnel l'infrastructure nécessaire au transfert de données de communication à des tiers. Les entreprises qui vendent des logiciels et des infrastructures de réseau en Suisse entrent, elles aussi, dans le champ d'application de la LSCPT dans la mesure où elles mettent à la

disposition des fournisseurs de services de télécommunication et d'autres entreprises l'infrastructure dont ils ont besoin en la leur vendant ou en la leur louant. Selon RD, ces exemples montrent qu'on n'a pas vraiment réfléchi aux conséquences qu'aurait l'extension du champ d'application de la LSCPT. Aussi demande-t-il qu'on renonce à cette dernière ou, du moins, qu'on étende le champ d'application de telle sorte que même en cas d'interprétation large de la disposition, ne soient visés que ceux qui doivent l'être.

CSI souligne que tous ses membres, à savoir les administrations publiques des trois niveaux étatiques, pourraient se retrouver soumis à la LSCPT du fait de cette disposition puisqu'ils exploitent généralement des réseaux téléphoniques et informatiques auxquels des tiers (p. ex., cantons, communes, autres autorités) se raccordent pour exécuter des tâches administratives. C'est pourquoi elle pense que cette disposition en général et son application aux réseaux des administrations publiques en particulier sont problématiques et demande la suppression de la let. b.

Dans sa prise de position, VD indique que le concept de « données de communication » utilisé à l'art. 2, al. 1, let. b, AP n'aide pas à déterminer précisément quelles sont les personnes visées par la let. b. A l'heure actuelle, la plupart des fournisseurs de services de télécommunication acceptent de livrer des données rétroactives directement aux services de police, voire sur requête d'un magistrat. On considère, en effet, qu'ils ne sont pas soumis au secret des télécommunications. VD se demande ce qu'il adviendra suite à la révision : les fournisseurs ne pourront-ils à l'avenir plus coopérer que dans les limites fixées par la LSCPT ?

EPFZ et UNISG attirent l'attention sur la contradiction suivante : tout d'abord, il est écrit dans le rapport explicatif que les « écoles » ne sont pas tenues d'exécuter des surveillances, puis il est dit dans le commentaire de l'art. 22 (Identification des utilisateurs qui accèdent à Internet) qu'elles y sont obligées. Il y a donc lieu de préciser à la let. b que seuls ceux qui fournissent des services pour les personnes mentionnées à la let. a sont inclus dans le champ d'application de la LSCPT. EPFZ exige, en outre, qu'en tant qu'établissement de droit public ne fournissant des services qu'à des étudiants et des organisations proches, elle ne soit pas soumise à la LSCPT, contrairement à ce que prévoit l'al. 1. Selon UNIZH, le terme de « personnes » ne permet pas vraiment de savoir si la loi s'applique aussi aux établissements. La formulation actuelle lui donne à penser qu'en tant qu'établissement cantonal, elle n'est pas concernée. Elle considère par ailleurs que la notion vague d'« activité à titre professionnel » ne s'applique pas à elle dans la mesure où elle est au service de la science. switch demande qu'on précise à la let. b que les écoles, les hautes écoles et les institutions qui, comme elle, sont chargées de fournir aux deux premières l'infrastructure (de réseau) dont elles ont besoin, ne soient pas soumises à la LSCPT.

1.2.3 Art. 2, al. 2 en relation avec l'art. 26

Art. 2, al. 2

[2] Les exploitants de réseaux de télécommunication internes et de centraux domestiques ainsi que les personnes mentionnées à l'al. 1 qui n'exercent pas leur activité dans le domaine de la correspondance par télécommunication à titre professionnel sont tenus de tolérer une surveillance au sens de la présente loi.

Art. 26 Exploitants de réseaux de télécommunication internes et de centraux domestiques et personnes visées à l'art. 2, al. 1, n'exerçant pas leur activité dans le domaine de la correspondance par télécommunication à titre professionnel

Les exploitants de réseaux de télécommunication internes et de centraux domestiques sont tenus d'en garantir l'accès aux personnes mandatées par le service. Les personnes mentionnées à l'art. 2, al. 1 qui n'exercent pas leur activité dans le domaine de la correspondance par télécommunication à titre professionnel sont tenues de garantir l'accès aux installations qu'elles utilisent aux personnes mandatées par le service. Les exploitants et les personnes précités sont tenus de fournir aux personnes mandatées par le service les renseignements nécessaires.

Quelques participants[50] proposent, sous la forme de normes rédigées, de préciser que l'art. 2, al. 1, AP ne s'applique pas aux écoles en tous genres, aux hôtels ni aux hôpitaux. EPFZ fait observer qu'elle doit être considérée comme une exploitante de réseaux de télécommunication internes et d'un central domestique au sens de l'al. 2. Conformément à l'art. 2, let. c, de l'ordonnance du 9 mars 2007 sur les services de télécommunication (OST)[51], elle n'est pas réputée fournir un service de télécommunication. Elle n'est pas non plus un fournisseur d'accès à Internet au sens où l'entend l'art. 2, let. a, de l'ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication (OSCPT)[52]. Les participants proposent de remplacer l'expression « n'exerçant pas leur activité dans le domaine de la correspondance par télécommunication à titre professionnel » par « n'exerçant pas d'activité commerciale à but lucratif dans le domaine de la correspondance par télécommunication ».

Au vu des sanctions pénales encourues et par souci d'assurer la sécurité du droit, LU propose de préciser qui sont les fournisseurs de services postaux et de télécommunication qui « n'exercent pas à titre professionnel ». Il demande, en outre, au même titre que BL, AR, PS et privatim, qu'on spécifie quelles sont les obligations concrètes incombant aux personnes désignées à l'al. 2. Selon SIUG, tous les particuliers et toutes les organisations et entreprises qui fournissent des services Internet à titre accessoire sont tenus de coopérer de manière passive et de mettre à disposition leurs locaux et leur équipement informatique, ce qui peut signifier que des mots de passe et des clés de cryptage doivent être divulgués et que des mesures d'écoute soient exécutées au moyen d'équipements privés. Il n'y a donc toujours pas lieu de soumettre les personnes qui n'exercent pas leur activité à titre professionnel à l'obligation de coopérer et de fournir des renseignements.

Selon CCC, l'art. 26 AP constitue une base légale permettant de s'introduire dans des locaux privés. Il est donc en contradiction avec l'art. 13 de la Constitution fédérale du 18 avril 1999 (Cst.) [53].

PPS ne voit pas un utilisateur d'Internet qui ne remplisse pas les conditions de l'art. 2, al. 2, AP. Tous les exploitants d'un LAN (y compris les particuliers) doivent tolérer une surveillance de la part de leur fournisseur d'accès à Internet.

Cablecom déplore que le renvoi à l'art. 2, al. 1, AP qui figure à l'art. 26 AP, ne soit pas correct dans la mesure où l'al. 1 ne s'applique clairement qu'à ceux qui exercent leur activité à titre professionnel. Un renvoi à l'art. 2, al. 2, AP serait plus juste à ses yeux.

1.3. Art. 3 Service de surveillance

[1] La Confédération exploite un service chargé de la surveillance de la correspondance par poste et télécommunication (service).

[2] Le service exécute ses tâches de manière autonome. Il n'est pas assujetti à des instructions et n'est rattaché au DFJP que sur le plan administratif.

[3] Dans l'exécution de ses tâches, il collabore avec les autorités concédantes et les autorités de surveillance compétentes en matière de services postaux et de télécommunications.

1.3.1 Art. 3, al. 1

[50] EPFZ, UNISG, asut, Swisscom, Finecom, Orange, Colt, Sunrise, Verizon, Swisscable, switch.
[51] RS 784.101.1
[52] RS 780.11
[53] RS 101

Pas de remarques.

1.3.2 Art. 3, al. 2

PDC souhaite que l'on mette fin au mélange des attributions du service, qui exécute à la fois des tâches normatives et des tâches d'exécution. ICT, ePower et SPICT trouvent tout simplement étonnant qu'un seul et même service intervienne sur mandat des autorités de poursuite pénale, édicte des normes d'exécution et puisse attribuer des certificats. Aussi demandent-ils une scission du service en deux entités. D'autres participants[54] relèvent que le service peut également remplir une fonction exécutive dans la mesure où il n'est pas assujetti à des instructions.

1.3.3 Art. 3, al. 3

ZH, LU, AG, CCPCS et PDC soulignent l'importance d'une étroite collaboration entre le service et les autorités de poursuite pénale. Celle-ci est impérative et doit donc être inscrite dans la loi en tant que mandat légal. La législation doit évoluer de pair avec les innovations technologiques. C'est la raison pour laquelle il faut ajouter « *de même qu'avec les autorités de poursuite pénale* » à l'al. 3. ICT, ePower et SPICT trouvent également frappant que la collaboration avec les autorités de poursuite pénale ne soit pas mentionnée à l'al. 3. Pour sa part, Cablecom ne comprend pas pourquoi le service ne doit avoir que la faculté et non l'obligation de fournir des conseils techniques en cas de problèmes. En tant que centre de compétence pour les surveillances, le service doit, s'il veut éviter les malentendus, transmettre son savoir aux fournisseurs. Cablecom propose donc un nouvel al. 4 qui aurait la teneur suivante : « Il est l'interlocuteur des autorités et des personnes tenues d'exécuter des surveillances sur les questions touchant aux mesures de surveillance et apporte son soutien à celles-ci en cas de problèmes. »

1.4. Art. 4 Traitement des données personnelles

Les autorités habilitées à ordonner ou à autoriser une surveillance de même que les personnes qui exécutent des surveillances en vertu de la présente loi peuvent traiter les données personnelles qui leur sont nécessaires pour assurer le suivi de l'exécution des ordres de surveillance.

Neuf participants[55] jugent la disposition sur le traitement des données personnelles inutile : le fait que les autorités de poursuite pénale, le service et les prestataires de services puissent traiter des données personnelles dans le but de poursuivre des infractions est une évidence.

Pour ZG, BL, PS et privatim, la clause générale que constitue l'art. 4 AP est illicite en tant qu'elle minimise l'exigence selon laquelle les données doivent être traitées dans un but déterminé. Dans le cadre des surveillances prévues par la LSCPT, des données personnelles sensibles peuvent également être traitées. En vertu de l'art. 17 de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[56], il faut que le type de données pouvant être traitées soit spécifié dans une disposition légale. Or l'art. 4 AP n'en fait aucune mention. Aux termes de l'art. 17 susmentionné, les données sensibles ou des profils de la personnalité ne peuvent être traités que si une loi au sens formel le prévoit expressément. Par conséquent, plus les données à traiter sont sensibles, plus la réglementation doit être précise. Cette dis-

---

54 asut, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
55 LU, NW, GL, GR, TG, VS, JU, CCDJP, CAPS.
56 RS 235.1

position générale n'empêche pas que le traitement de données personnelles sensibles et de profils de personnalité se fonde sur une autre disposition légale expresse qui satisfait au principe de précision. BS et VD souhaitent, eux aussi, que cette disposition soit précisée. NE demande, en outre, qu'on édicte des dispositions concernant la destruction de données inutiles ou recueillies par erreur ou qu'au moins on renvoie à la LPD.

Neuf participants[57] relèvent que les principes posés par l'art. 4 LPD tels que la proportionnalité, la bonne foi ou le traitement des données dans un but déterminé doivent être respectés. Une grande majorité d'entre eux[58] a proposé le nouveau libellé suivant : « Les autorités habilitées à ordonner ou à autoriser une surveillance de même que les personnes qui exécutent des surveillances en vertu de la présente loi peuvent traiter les données personnelles qui leur sont nécessaires pour assurer le suivi de l'exécution des ordres de surveillance *légitimes* qui leur ont été *donnés par un tribunal*. *Les principes posés par la loi fédérale sur la protection des données doivent, par ailleurs, être respectés. »*

Kf craint que des personnes intègres soient surveillées et que les données les concernant soient conservées pendant des années.

1.5. Art. 5 Secret des postes et des télécommunications

La surveillance et toutes les informations qui s'y rapportent sont soumises au secret des postes et des télécommunications au sens de l'art. 321ter CP.

Quelques participants[59] soulignent qu'il est déjà question du secret des télécommunications à l'art. 43 de la loi du 30 avril 1997 sur les télécommunications (LTC) [60]. L'évoquer dans la LSCPT pourrait donc prêter à confusion car on pourrait supposer que les données contenant des « renseignements sur des raccordements » sont couvertes par ce secret. Par ailleurs, contrairement à ce que laisse à penser le libellé de la disposition, ce n'est pas la « surveillance » qui est principalement soumise au secret des télécommunications mais, d'une manière générale, toutes les communications qui transitent par les réseaux de télécommunication publics. La surveillance ne justifie donc pas le secret des télécommunications ; elle constitue plutôt une violation de ce dernier. Selon RD, cette disposition implique, d'une manière générale, que des informations qui ne sont normalement pas couvertes par le secret des télécommunications le soient du fait de cette disposition.

2. Système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication

2.1. Art. 6 Principe

Le service exploite un système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication visée à l'art. 1, al. 1 (système de traitement).

SH s'oppose à une conservation centralisée et durable des données au sein du service. ICT et ePower pensent, au contraire, que la centralisation du stockage des données constitue un progrès manifeste qui permettra de réduire les coûts liés au processus de surveillance.

IT(19) demande que cette disposition soit complétée par des règles claires en ce qui

---

57 USS, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
58 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
59 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
60 RS 784.10

concerne la nécessité de contrôler toutes les données recueillies lors d'une surveillance et par des définitions précises de toutes les tâches à effectuer par le service. Si l'introduction de programmes informatiques est une fonctionnalité du système informatique, PPS demande que la question du traitement des systèmes informatiques surveillés soit également réglée dans cette disposition. Si ce n'est pas le cas, il convient de prévoir une disposition légale qui définira cette tâche.

JDS et droitsfondamentaux.ch exigent que le système de traitement soit conçu de façon à garantir aux personnes concernées le droit de consulter leur dossier et d'accéder aux données les concernant. Le commentaire de cet article dans le rapport explicatif n'est pas sans susciter certaines réserves à ce sujet.

De l'avis de CP, le système de traitement doit être sécurisé au maximum en raison du risque élevé d'attaques électroniques dont il peut faire l'objet.

2.2. Art. 7 But du système de traitement

[1] Le système de traitement sert à:

a. centraliser la conservation des données recueillies lors de la surveillance de la correspondance par télécommunication;

b. consulter en ligne ces données selon l'art. 9.

Six participants[61] sont favorables à un système de mise à disposition centralisée des données. La nouvelle réglementation ne doit toutefois pas exclure la possibilité que les données soient, en cas de besoin, enregistrées sur d'autres supports de données et mises à la disposition des autorités ayant ordonné une surveillance. Ce procédé est nécessaire, comme on peut le constater dans la pratique, et il le restera, en particulier dans le cadre de l'entraide judiciaire internationale, car c'est par ce seul biais que la transmission des données aux tribunaux reste possible.

Pour CAPS, les données recueillies lors de surveillances téléphoniques n'ayant rien révélé de suspect ne doivent à l'avenir pas être conservées au sein du service. Elles doivent rester stockées sur des supports de données dans le dossier pénal. Elle demande, par conséquent, que le but du système de traitement soit revu.

ZG, BL et privatim estiment qu'au regard du droit constitutionnel et de celui de la protection des données, la centralisation de la conservation des données est un moyen et non une fin en soi. ZG demande que l'art. 7, al. a, AP soit modifié en conséquence. BL pose la question de savoir s'il ne faut pas justifier la centralisation de la conservation par un autre but et privatim propose la formulation suivante : « La centralisation dans le système de traitement de la conservation des données recueillies lors de la surveillance de la correspondance par télécommunication sert à consulter en ligne ces données conformément à l'art. 9 AP. »

Quelques participants[62] déplorent que ne soit pas indiqué dans la disposition proposée que le but premier du système de traitement est la réception de données et proposent un nouveau libellé tenant compte de cette critique.

ISSS pense que, pour garantir la protection des droits fondamentaux et de la sphère privée et pour prévenir les risques d'abus, un système centralisé doit obligatoirement faire l'objet

---

61 ZH, GL, VS, JU, CCDJP, CCPCS.

62 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, Cablecom.

d'un contrôle de la part d'une autorité indépendante, comme le Préposé fédéral à la protection des données et à la transparence.

2.3. Art. 8 Contenu du système de traitement

Le système de traitement contient:

a. les communications de la personne surveillée, y compris celles reçues;

b. les données indiquant quand et avec quels raccordements la personne surveillée a été ou est en liaison par télécommunication et les données relatives au trafic et à la facturation.

Plusieurs participants[63] préconisent que l'art. 8, let. b, AP mentionne expressément les renseignements géographiques. CCPCS estime que les tentatives d'établissement de liaisons peuvent également s'avérer importantes et demande donc qu'il en soit question dans la loi. LU, SG, BL, NW et CAPS exigent que la let. b soit formulée plus clairement, notamment que soit spécifiée la différence entre les données permettant l'identification des usagers et les données relatives au trafic et à la facturation. NW, SG et CAPS souhaitent une formulation plus claire de l'art. 273 CPP, allant dans le même sens. BL émet le même souhait en ce qui concerne l'art. 16, let. e, AP.

Considérant que l'art. 7 AP constitue une disposition de principe suffisante, certains participants[64] demandent que l'art. 8 AP, qui est superflu à leurs yeux, soit biffé. Cablecom estime que la let. a est inutile et que sa formulation est équivoque. Il ne voit pas pourquoi les communications reçues sont expressément mentionnées et non les communications émises. La let. b est impossible à appliquer à la correspondance par Internet.

2.4. Art. 9 Accès au système de traitement

[1] Le service permet aux autorités ayant ordonné une surveillance et aux personnes désignées par celles-ci, dans les limites de l'autorisation qui leur est octroyée, d'accéder en ligne aux données recueillies lors de la surveillance considérée contenues dans le système de traitement.

[2] L'autorité ayant ordonné une surveillance et les personnes désignées par celle-ci au sens de l'al. 1 ont accès en ligne aux données recueillies lors de la surveillance considérée aussi longtemps que l'autorité ayant ordonné cette surveillance est saisie du dossier, mais pendant une année au plus depuis la fin de la surveillance. L'autorité ayant ordonné une surveillance informe le service de son dessaisissement du dossier et de la fin de la surveillance; les art. 274, al. 5 et 275 CPP sont réservés. L'autorité ayant ordonné une surveillance et encore saisie du dossier peut demander au service la prolongation de l'accès aux données pour des périodes n'excédant pas une année. Le service informe cette autorité de l'échéance prochaine du délai d'accès en ligne aux données.

[3] L'autorité ayant ordonné une surveillance qui est dessaisie du dossier informe le service, cas échéant, de l'autorité nouvellement saisie du dossier.

[4] Le service permet à l'autorité nouvellement saisie du dossier qui lui en fait la demande et aux personnes désignées par celle-ci, dans les limites de l'autorisation qui leur est octroyée, d'accéder en ligne aux données recueillies lors de la surveillance considérée contenues dans le système de traitement. L'autorité nouvellement saisie du dossier et les personnes désignées par celle-ci ont accès en ligne à ces données aussi longtemps que l'autorité nouvellement saisie du dossier demeure en charge de celui-ci, mais pendant une année au plus depuis sa demande d'accès adressée au service. Pour le surplus, les al. 2 et 3 sont applicables par analogie.

[5] Si, pour des raisons techniques, la consultation en ligne des données recueillies lors de la surveillance considérée n'est pas possible, ces données sont communiquées au moyen d'envois postaux de supports de données et de documents.

Neuf participants[65] préconisent de mentionner expressément à l'al. 5 le fait que les données peuvent devoir être communiquées au moyen d'envois postaux de supports de données et de documents, dans certaines circonstances particulières ou pour des raisons techniques.

---

63 ZH, AG, TI, GL, TG, VS, JU, CCDJP, CCPCS.

64 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

65 ZH, AG, GL, TG, VS, JU, CCDJP, CCPCS, CCC.

De plus, afin de prévenir abus, extorsions et chantages, les parties à une procédure, en particulier la défense, ne doivent avoir accès aux données qu'en utilisant le raccordement du ministère public ou du juge d'instruction compétent. Il faut éviter, p. ex., au moyen du cryptage, que des personnes puissent consulter ces données sans y être autorisées. VD considère que l'accès en ligne peut être une solution envisageable à condition qu'elle garantisse aux parties et aux tribunaux le même accès aux données qu'aujourd'hui.

BE, NW, BL et SSDP souhaitent conserver l'ancien système. La réglementation proposée est compliquée, ne tient pas compte du risque de dysfonctionnement et est inutile. Aujourd'hui, il est possible de se dessaisir d'un dossier, de joindre des procédures ou d'en conduire séparément. Or le nouveau système ne tient pas compte de ces différentes possibilités. La réglementation proposée est, par ailleurs, parfois en contradiction avec le CPP, conformément auquel les parties doivent avoir accès aux originaux. Le fait que les parties puissent directement avoir accès au système du service appelle des réserves sous l'angle de la sécurité. Le nouveau système présente de gros inconvénients mais pas d'avantages notables. LU, SZ, SO, SG, SH et CAPS souhaitent, eux aussi, conserver l'ancien système et demandent que l'on examine s'il ne serait pas judicieux de limiter la conservation centralisée des données à Internet en raison de la quantité astronomique de données recueillies et de continuer à enregistrer et à envoyer, comme c'est le cas aujourd'hui, les surveillances téléphoniques sur des supports de données. LU se pose la question de savoir si ces données seront encore disponibles au cas où elles devraient être consultées ultérieurement, dans le cadre d'une révision du jugement pénal, le rapport explicatif ne le garantissant pas. ZG souhaite une simplification de la réglementation. BS, FSA et MS estiment que le système proposé porte atteinte aux droits des parties et qu'un mécanisme de surveillance visant à garantir que toutes les données pertinentes figurent dans le dossier, serait nécessaire.

PDC attire l'attention sur les risques d'abus existant dans le domaine d'Internet et souhaite qu'on garantisse le fait qu'on ne puisse consulter que les données ayant été recueillies lors de la surveillance.

Pour certains participants[66], le renvoi à la loi sur la protection des données à l'art. 10, al. 2, AP intervient beaucoup trop tard. Les données doivent être protégées dès lors qu'elles ont été recueillies. En outre, l'al. 1 ne spécifie pas qui est habilité à octroyer l'autorisation. Par ailleurs, cet article ne prévoit aucun mécanisme visant à garantir la protection des données, ce qui est regrettable pour ces participants.

2.5. Art. 10 Droit de consulter le dossier et droit d'accès aux données

[1] Le droit de consulter le dossier et le droit d'accès aux données de la personne concernée par les données recueillies dans le cadre d'une procédure pénale (art. 1, al. 1, let. a) sont régis par les art. 95, 97, 98, 99, al. 1, 101, al. 1, 102 et 279 CPP.

[2] Le droit de consulter le dossier et le droit d'accès aux données de la personne concernée par les données recueillies lors de l'exécution d'une demande d'entraide (art. 1, al. 1, let. b) sont régis par la législation spéciale dans cette matière ainsi que soit par la loi fédérale du 19 juin 1992 sur la protection des données (LPD), si l'autorité saisie de la demande d'entraide est une autorité de la Confédération, soit par le droit cantonal, si cette autorité est le ministère public d'un canton.

[3] Le droit de consulter le dossier et le droit d'accès aux données de la personne concernée par les données recueillies lors de la recherche de personnes disparues (art. 1, al. 1, let. c) ou lors de la recherche de personnes condamnées (art. 1, al. 1, let. d) sont régis par le droit cantonal. L'article 29 est réservé.

[4] La personne concernée par les données recueillies lors de la surveillance considérée fait valoir ses droits auprès de l'autorité en charge du dossier. S'il n'y a plus d'autorité en charge du dossier, elle doit les faire valoir au-

66 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

près de la dernière à l'avoir été ou de celle qui a succédé à celle-ci. La personne concernée ne peut faire valoir ses droits auprès du service.

Un grand nombre de participants[67] rejette l'art. 10 au motif que le CPP contient suffisamment de dispositions visant à protéger les données personnelles. Le principe énoncé à l'al. 1 selon lequel le droit de consulter le dossier et le droit d'accès aux données sont régis par le CPP, est une évidence. Les articles du CPP auxquels renvoie l'al. 1 ne sont cependant pas pertinents dans le cadre de surveillances secrètes. BL, qui est de cet avis, demande donc une adaptation de cette disposition qui tienne compte de cette remarque. L'introduction à l'al. 2 d'une compétence suisse pour les demandes émanant de l'étranger n'a aucun sens. L'art. 279 CPP est tout à fait applicable par analogie aux recherches dans les cas d'urgence visées par l'al. 3. La référence au droit cantonal dans l'al. 3 n'a aucun sens selon les participants susmentionnés. SZ, au contraire, la trouve appropriée. L'al. 4 est considéré comme inutile.

De l'avis de FR, les tiers non impliqués dans la procédure doivent avoir le droit de consulter les données qui les concernent.

PPS déplore que le droit conféré par l'al. 4 ne profite à personne lorsque la surveillance est exécutée de manière discrète ou lorsqu'on a renoncé à la communication conformément à l'art. 279, al. 2, CPP.

2.6. Art. 11 Délai de conservation des données

[1] Les données recueillies dans le cadre d'une procédure pénale (art. 1, al. 1, let. a) sont conservées dans le système de traitement jusqu'à l'expiration du délai de prescription de l'action pénale. L'autorité en charge du dossier communique au service quel est ce délai.

[2] Les données recueillies lors de l'exécution d'une demande d'entraide (art. 1, al. 1, let. b) sont conservées dans le système de traitement aussi longtemps que le but poursuivi l'exige, mais trente ans au plus.

[3] Les données recueillies lors de la recherche de personnes disparues (art. 1, al. 1, let. c) sont conservées dans le système de traitement aussi longtemps que le but poursuivi l'exige, mais trente ans au plus.

[4] Les données recueillies lors de la recherche de personnes condamnées à une peine privative de liberté (art. 1, al. 1, let. d) sont conservées dans le système de traitement aussi longtemps que le but poursuivi l'exige, mais au plus tard jusqu'à l'expiration du délai de prescription de la peine. L'autorité en charge du dossier communique au service quel est ce délai. Les données recueillies lors de la recherche de personnes qui font l'objet d'une mesure entraînant une privation de liberté (art. 1, al. 1, let. d) sont conservées aussi longtemps que le but poursuivi l'exige, mais trente ans au plus.

[5] La Confédération et chaque canton désignent une autorité que le service informe de l'échéance prochaine du délai de conservation des données considérées. Cette autorité transmet l'avis à l'autorité en charge du dossier ou, s'il n'y a plus d'autorité en charge du dossier, à la dernière à l'avoir été ou à celle qui a succédé à celle-ci. A l'expiration du délai de conservation des données considérées dans le système de traitement, l'autorité qui a reçu cet avis demande au service de lui transférer ces données. Une fois que ce transfert a été effectué ou en l'absence d'une telle demande, le service détruit les données considérées du système de traitement.

Plusieurs participants[68] rejettent l'art. 11 AP en faisant valoir que la conservation du système actuel qu'ils revendiquent, rendrait obsolète la réglementation des délais de prescription et de conservation, qu'ils jugent compliquée. Ils préfèrent le système actuel, dans lequel le sort des données suit celui des autres pièces du dossier, à une réglementation spéciale. Cet article n'a de sens que dans la mesure où les données sont conservées au sein du service et non dans le dossier pénal, ce qui n'est pas judicieux. Le fait de faire dépendre les délais de conservation des données de la prescription de la poursuite pénale est confus et générera une charge administrative inutile. Le système d'annonce qui est proposé est trop compliqué ; l'ensemble de la procédure est trop complexe et coûteux. Les délais de conservation de-

67 LU, NW, BL, SG, GL, TG, VS, JU, CCDJP, CAPS, SSDP.
68 BE, SZ, NW, BL, SH, SG, AG, VD, CAPS.

vraient être fixés d'après le CPP, car il n'est pas judicieux d'avoir plusieurs réglementations sur lesquelles s'appuyer. Pour CAPS, il suffirait, dans le cas où l'on déciderait de mettre en place le système proposé, d'ajouter une disposition prévoyant que l'autorité en charge du dossier s'assure, une fois le délai de conservation expiré, que les données conservées au sein du service soient détruites. AG voudrait que le délai de conservation des données soit le même dans tous les cas de figure (p. ex., 10 ou 15 ans).

ZG souhaite que l'on précise le libellé de l'al. 1 de manière à ce qu'il soit statué clairement qui doit communiquer au service le délai de prescription de l'action pénale.

PDC, PES, JDS et droitsfondamentaux.ch trouvent les délais de conservation prévus par l'art. 11 AP beaucoup trop longs. PDC demande donc que ces délais soient raccourcis. PES, JDS et droitsfondamentaux.ch exigent que les données soient transférées au plus tard au terme de la procédure pénale et ne soient conservées qu'en vue de permettre aux personnes concernées de les consulter. Dès lors que la procédure est close, rien ne s'oppose à ce que ces dernières consultent toutes les données les concernant. Voilà pourquoi il faut que tous les enregistrements leur soient automatiquement remis dans un format courant.

PPS préconise qu'à expiration du délai de conservation prévu par l'al. 1 les données soient détruites. Contrairement à ce qui est proposé, ce n'est pas le but poursuivi qui doit être déterminant pour la fixation de ce délai mais la prescription.

IT(19), ISSS, hp et COG demandent que soit spécifié à l'art. 11 quelle autorité décide, dans chaque cas, de la durée effective de la conservation des données. Ils souhaitent par ailleurs que les conditions de la destruction immédiate des données qui ne sont plus nécessaires à l'exécution de la surveillance et la procédure en la matière soient définies et qu'un contrôle visant à garantir la destruction effective des données soit prévu.

Huit participants[69] proposent que l'al. 5 soit complété comme suit: « …du système de traitement et de tous les autres dispositifs de sauvegarde… ».

2.7. Art. 12 Sécurité

Le service est responsable de la sécurité du système de traitement. Le Conseil fédéral édicte les dispositions relatives aux mesures de protection techniques et organisationnelles, en particulier contre l'accès, la modification, la diffusion non autorisée et la destruction accidentelle ou non autorisée de données. Les personnes qui exécutent des surveillances en vertu de la présente loi sont tenues de se conformer aux instructions du service en matière de sécurité des données lors de la transmission des données résultant d'une surveillance.

IT(19) demande que l'art. 12 AP soit complété par des règles claires en ce qui concerne la nécessité de contrôler toutes les données résultant d'une surveillance et par des définitions précises des tâches à effectuer par le service.

SWICO, hp et COG se demandent quelles charges et obligations les dispositions relatives aux mesures de protection techniques et organisationnelles que le Conseil fédéral doit édicter engendreront pour les fournisseurs de services de télécommunication et les fournisseurs de services Internet, qui sont également visés par l'art. 12, et quel coût elles généreront. Ils souhaitent que ces charges et obligations n'entraînent aucun coût supplémentaire.

PPS propose que les dispositions relatives aux mesures de protection technique et organisa-

[69] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

tionnelle ne s'appliquent pas seulement au service et aux personnes qui exécutent des surveillances, mais aussi aux autorités qui utilisent le système de traitement et aux services ayant été désignés par ces dernières.

2.8. Art. 13 Responsabilité

Les autorités ayant accès au système de traitement (art. 9) sont les maîtres du fichier pour ce qui concerne les données recueillies lors de surveillances relevant de leur compétence.

Quelques participants[70] ont proposé la modification suivante : « Les autorités *ayant ordonné des surveillances et ayant* accès au système de traitement (art. 9) *veillent à ce que le fichier soit utilisé conformément à la loi* pour ce qui concerne les données recueillies lors de surveillances relevant de leur compétence ». Cablecom préconise, quant à lui, la précision suivante : « Les autorités *ayant ordonné des surveillances* sont les maîtres du fichier pour ce qui concerne les données recueillies lors de surveillances relevant de leur compétence ».

3. Tâches du service

3.1. Art. 14 Renseignements sur les raccordements de télécommunication

Le service fournit des renseignements sur les données mentionnées à l'art. 20, al. 1 à 3 exclusivement aux autorités et aux fins suivantes lorsque celles-ci le demandent:

a. aux autorités fédérales et cantonales qui peuvent ordonner ou autoriser une surveillance de la correspondance par télécommunication, pour déterminer les raccordements et les personnes à surveiller;

b. à l'Office fédéral de la police et aux commandements des polices cantonales et municipales, pour exécuter des tâches de police;

c. aux autorités fédérales et cantonales compétentes, pour régler des affaires relevant du droit pénal administratif.

safe relève que, conformément à l'art. 14, al. 2 en relation avec l'al. 4, LSCPT, l'identité du titulaire d'un raccordement peut être divulguée dans le cadre d'une procédure simplifiée. Selon le rapport explicatif, cette disposition est reprise en substance à l'art. 14 AP en relation avec l'art. 20, al. 3, AP. La possibilité d'obtenir des renseignements en passant par une procédure simplifiée est offerte, conformément à l'art. 14, al. 2, let. b et c, LSCPT, non seulement aux autorités de police pour exécuter des tâches de police et aux autorités administratives pour régler des affaires relevant du droit pénal administratif mais aussi, conformément à l'art. 14, al. 2, let. b, aux autorités fédérales et cantonales, mais uniquement celles qui peuvent ordonner ou autoriser une surveillance de la correspondance par télécommunication (art. 6 LSCPT, autorités de poursuite pénale), dans le seul but de déterminer les raccordements et les personnes à surveiller. Selon safe, l'utilisation de ces données dans un but déterminé se trouve ainsi limitée aux surveillances ordonnées en vue de poursuivre les infractions prévues par l'art. 269, al. 2, let. a, CPP, ce que ne peut avoir souhaité le législateur. Toutes les autorités de poursuite pénale devraient pouvoir obtenir ces renseignements par voie simplifiée afin de poursuivre les infractions commises sur Internet, mais aussi et surtout de conserver des preuves de ces dernières. La divulgation de l'identité du titulaire d'un raccordement est indispensable pour prévenir efficacement la criminalité. Aussi safe demande-t-il que l'art. 14, let. a, AP soit modifié comme suit : « les autorités fédérales et cantonales de poursuite pénale, pour poursuivre les infractions et prévenir la criminalité. »

[70] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

3.2. Art. 15 Tâches générales dans le domaine de la surveillance

Dans les domaines de la surveillance de la correspondance par poste et télécommunication, les tâches générales du service sont les suivantes:

a. il vérifie que la surveillance concerne une infraction pouvant faire l'objet d'une telle mesure en vertu du droit applicable et qu'elle a été ordonnée par l'autorité compétente; si l'ordre de surveillance est clairement erroné ou qu'il n'est pas motivé, le service prend contact avec l'autorité habilitée à autoriser la surveillance avant que des envois ou des informations ne soient transmis à l'autorité qui a ordonné la surveillance;

b. il donne aux personnes qui exécutent des surveillances de la correspondance en vertu de la présente loi des directives sur la mise en œuvre de la surveillance, leur demande de prendre toute mesure utile à cette mise en œuvre et en contrôle l'exécution;

c. il met en œuvre les mesures visant à protéger le secret professionnel qui ont été ordonnées par l'autorité qui a autorisé la surveillance;

d. il vérifie que la surveillance ne s'étend pas au-delà de la durée autorisée et y met fin à l'expiration du délai si aucune demande de prolongation n'a été déposée;

e. il communique immédiatement la levée de la surveillance à l'autorité qui l'a autorisée.

Quelques participants[71] souhaitent l'adjonction d'une let. f à l'art. 15 AP qui aurait la teneur suivante : « il fournit aux autorités et aux fournisseurs de services de télécommunication des conseils techniques en matière de surveillance de la correspondance par télécommunication ».

PPS déplore que la disposition ne fasse pas mention des tâches générales du service en matière d'élaboration et de maintenance des systèmes d'infiltration (v. infra, partie III, ch. 11.1.2, remarques concernant l'art. 270bis CPP).

3.2.1 let. a

PLR demande que le rôle du service, notamment en ce qui concerne ses compétences vis-à-vis des autorités de poursuite pénale, soit d'une manière générale défini plus clairement.

Un nombre non négligeable de participants[72] souligne que le service n'a pas la compétence de vérifier la légalité des surveillances ordonnées. Dans la pratique, le service se borne à transmettre les ordres de surveillance même si ceux-ci sont clairement erronés. S'ajoute à cela le fait que les personnes tenues d'exécuter des surveillances ne peuvent recourir contre une mesure de surveillance en invoquant son illégalité (v. propositions similaires dans la partie III, ch. 9.2, remarque concernant l'art. 34 AP « Voies de droit »). Le Tribunal administratif fédéral ne peut examiner les faits en sa qualité d'instance de recours que si le service les a examinés en première instance. Or, cette condition fait défaut. La modification suivante est donc proposée : « a. il vérifie que la surveillance a été ordonnée par l'autorité compétente, que le type de mesure ordonné est prévu par la loi et qu'il est possible à exécuter sur le plan technique et organisationnel. Il ne vérifie pas que l'ordre de surveillance en question respecte les exigences de l'art. 269, let. b et c, du code de procédure pénale et que la mesure est conforme au principe de la proportionnalité ». BL relève que si la faisabilité technique et organisationnelle d'une mesure constitue un motif de recours au sens de l'art. 34, al. 2, LSCPT, il y a lieu d'examiner celle-ci avant d'ordonner une surveillance. Aussi l'art. 15, let. a, AP doit-il être complété en conséquence (v. infra, partie III, ch. 9.2.2, remarques concernant l'art. 34, al. 2, AP).

Quelques participants[73] demandent par ailleurs que l'on ajoute la phrase suivante à la let. a :

---

71 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.

72 Swisscable, SWICO, SKS, Cablecom, asut, Orange, Swisscom, Colt, Sunrise, Verizon, CAPS, economiesuisse, PES, SKS, IT(19).

73 asut, Orange, Swisscom, Colt, Sunrise, Verizon.

« En cas de doute quant à l'existence d'une obligation d'exécuter une surveillance, il tranche par voie de décision en application des dispositions légales pertinentes ». La plupart d'entre eux posent la question de savoir si le service est habilité à prendre des décisions à l'encontre des fournisseurs de services de télécommunication car la notion de décision présuppose que celui qui prend la décision examine cette dernière sous l'angle juridique et la motive. Cablecom attire par ailleurs l'attention sur la contradiction existant avec l'art. 33 AP, qui statue que le service veille à ce que la législation relative à la surveillance de la correspondance par poste et télécommunication soit respectée.

3.2.2 let. b

Plusieurs fournisseurs[74] de services de télécommunication proposent que la let. b soit complétée comme suit : « il donne, *dans le cadre des dispositions légales pertinentes*, des directives sur la mise en œuvre de la surveillance aux personnes qui exécutent des surveillances de la correspondance en vertu de la présente loi, leur demande de prendre toute mesure utile à cette mise en œuvre et en contrôle l'exécution ».

3.2.3 let. c à e

Pas de remarques.

3.3. Art. 16 Tâches dans le domaine de la surveillance de la correspondance par télécommunication

Dans le domaine de la surveillance de la correspondance par télécommunication, les tâches du service sont en outre les suivantes:

a. *il prend contact, dans les plus brefs délais, avec l'autorité qui a ordonné la surveillance et avec l'autorité habilitée à autoriser la surveillance s'il estime que celle-ci n'est techniquement pas possible à exécuter ou que son exécution est liée à des difficultés importantes;*

b. *il confie la surveillance à la personne exécutant des surveillances de la correspondance par télécommunication en vertu de la présente loi qui est préposée à la gestion du numéro d'appel ou à celle à laquelle l'exécution technique de la surveillance occasionne la moins grande charge, lorsque plusieurs personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi participent à l'exploitation du service de télécommunication à surveiller;*

c. *il reçoit les communications de la personne surveillée qui ont été déviées par les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi; il les enregistre et en permet la consultation à l'autorité qui a ordonné la surveillance;*

d. *il ordonne aux personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi de transmettre les communications de la personne surveillée directement au service de police désigné par l'autorité qui a ordonné la surveillance, si, pour des raisons techniques, il n'est pas en mesure de recevoir, d'enregistrer ou de transmettre ces communications à l'autorité qui a ordonné la surveillance;*

e. *il reçoit des personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi les données indiquant quand et avec quels raccordements la personne surveillée a été ou est en liaison par télécommunication et les données relatives au trafic et à la facturation; il les enregistre et en permet la consultation à l'autorité qui a ordonné la surveillance;*

f. *il ordonne, à la demande de l'autorité qui a ordonné la surveillance, aux personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi de ne transmettre que certains types de données composant le flux de données considéré.*

3.3.1 let. a

CAPS salue expressément le pragmatisme du mécanisme proposé. Pour ZH et CAPS, la formulation de la let. a ne garantit pas que le service examine en détail la faisabilité de la mesure. Ils proposent donc la formulation suivante : « s'il en arrive à la conclusion, après un

[74] asut, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

examen approfondi,... ».

Plusieurs participants[75] pensent qu'une reformulation correcte de l'art. 15, let. a, AP (v. supra, partie III, ch. 3.2.1, remarques concernant l'art. 15, let. a, AP) rendrait l'art. 16, let. a, AP obsolète.

Cablecom se demande où le service va pouvoir aller chercher des connaissances approfondies sur toutes les technologies qui lui permettront de juger que l'exécution d'une surveillance sera liée à des difficultés importantes. Aussi propose-t-il que, dans certains cas, les personnes impliquées se rassemblent autour d'une table pour discuter des possibilités et des conséquences.

3.3.2 let. b

privatim considère que l'expression « gestion du numéro d'appel » ne convient pas dans le contexte de la correspondance par Internet et propose donc de la remplacer par « gestion du raccordement ».

Six participants[76] proposent sous la forme de normes rédigées que le mandat de surveillance soit automatiquement confié à l'entreprise qui fournit des services à l'usager à surveiller.

Cablecom attire l'attention sur le fait que, conformément à cette disposition, un fournisseur peut être contraint d'exécuter des tâches qui avaient été confiées à une autre personne tenue d'exécuter une surveillance si le service estime qu'il remplira mieux ses obligations. Les critères sur lesquels le service se fonde pour prendre sa décision ne sont toutefois pas clairs. Compte tenu du fait que les surveillances ne seront plus indemnisées, des disparités économiques vont se faire jour. Il y a, en effet, de fortes chances que les gros fournisseurs exécutent des mandats en lieu et place des petits étant donné qu'ils sont techniquement mieux à même d'effectuer des surveillances. Cablecom propose donc que le mandat de surveillance soit confié à la personne qui fournit des services de télécommunication à l'usager à surveiller.

3.3.3 let. c

Pas de remarques.

3.3.4 let. d

Quelques participants[77] se félicitent expressément de cette disposition. Des participants appartenant à la branche des télécommunications[78] plaident, au contraire, pour une suppression de la let. d. Ils estiment, en effet, que le service de surveillance doit toujours être en mesure de recevoir les communications dans la mesure où on exige bien des fournisseurs de services de télécommunication qu'ils remplissent leurs obligations. Pour FSA, le branchement direct doit rester une exception.

3.3.5 let. e

---

75 asut, Orange, Swisscom, Colt, Sunrise, Finecom.
76 asut, Finecom, Orange, Swisscom, Colt, Sunrise.
77 AG, GL, GR, TG, JU, CAPS, CCDJP.
78 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Cablecom.

De l'avis de plusieurs participants[79], les données permettant l'identification des usagers ne doivent à l'avenir pas non plus transiter par le système de surveillance ISS[80]. La solution actuelle qui consiste, pour les fournisseurs de services de télécommunication, à mettre les données directement à la disposition des autorités chargées de les exploiter, ne pose, pour certains d'entre eux, qu'un problème : les données ne sont pas livrées dans un format standard. Ce problème peut toutefois être résolu simplement par le biais de directives techniques. BL souhaite, lui aussi, que les données soient livrées dans un format standard et exige qu'on explique dans la loi la différence – si tant est qu'il en existe une – entre les « données permettant l'identification des usagers » et les « données relatives au trafic et à la facturation ».

3.3.6 let. f

Plusieurs participants appartenant à la branche des télécommunications[81] pensent que le filtrage des données composant le flux considéré doit incomber à l'autorité qui a ordonné la surveillance ou au service et préconisent donc la suppression de cette disposition (v. aussi infra, partie III, ch. 5.2.3, remarques concernant l'art. 21, al. 3, AP). Cablecom demande également la suppression de cette disposition au motif qu'un filtrage des données par les fournisseurs de services de télécommunication peut entraîner des failles dans la surveillance. Il se peut, en effet, que des données soient irrémédiablement perdues. Le filtrage doit être effectué par les autorités d'instruction qui s'occupent du cas en question.

3.4. Art. 17 Contrôle de qualité

[1] Le service prend les mesures de contrôle préventives et ultérieures relatives à la qualité des données livrées par les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi.

[2] Le contrôle de qualité ne peut être effectué qu'avec l'accord préalable de l'autorité qui a ordonné la surveillance si le service doit pour ce faire avoir connaissance du contenu de ces données.

FSFP considère cette disposition comme très importante. Le contrôle de qualité doit être garanti et effectué régulièrement. Ce participant demande donc qu'en cas de non-respect des exigences posées, des sanctions claires soient prises, comme un retrait de la concession. KFG, par contre, ne voit pas bien le but de cette disposition. Un contrôle de qualité n'a de sens que si l'on peut passer au crible l'ensemble des données. Aussi la disposition doit-elle être précisée ou biffée.

3.5. Art. 18 (en relation avec l'art. 24) Certification

Art. 18:

Le service octroie, contre paiement, aux fournisseurs de services de télécommunication un certificat attestant qu'ils sont en mesure d'exécuter une surveillance correctement. Le service fixe les modalités de la certification.

Art. 24:

Les fournisseurs de services de télécommunication qui n'ont pas de certification prennent à leur charge les frais liés à l'éventuelle nécessité de recourir au service ou à un tiers pour la bonne exécution d'une surveillance. Dans ce cas, ils doivent sans tarder entreprendre les démarches pour obtenir une certification, délivrée par le service, conformément à l'art. 18.

---

79 NW, AG, GL, GR, TG, JU, CCDJP.
80 Interception System Schweiz.
81 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.

Un nombre non négligeable de participants[82] juge qu'une certification serait, sur le principe, judicieuse. Ils demandent cependant que soit instaurée l'obligation d'obtenir un certificat attestant que les nouveaux services proposés sont soumis à surveillance.

VD pense que l'AP n'expose pas clairement quelle est la finalité précise de la certification et pose la question de savoir s'il ne serait pas judicieux de préciser que la valeur d'un moyen de preuve n'est pas liée à la certification.

Citant l'exemple de l'Allemagne, ZH et CCPCS proposent que les fabricants d'équipement de télécommunication se fassent certifier. Ils estiment, d'une part, que la certification des fournisseurs de services de télécommunication serait très coûteuse et, d'autre part, qu'il serait plus simple de reprendre, dans le cadre de la collaboration européenne, un certificat existant. Pour CCPCS, la certification des fabricants offrirait davantage de sécurité juridique aux fournisseurs et une meilleure protection de l'innovation.

Plusieurs participants appartenant à la branche des télécommunications[83] soulignent qu'une certification n'aura aucun sens tant que les obligations des fournisseurs de services de télécommunication ne seront pas suffisamment bien définies et qu'elles ne connaîtront aucune limite du fait de l'absence de moyen de recours efficace contre les nouvelles méthodes de surveillance. Dans ces conditions, le certificat n'aura de valeur qu'au moment où il est obtenu et n'en aura absolument aucune par la suite. Les participants susmentionnés proposent donc de reformuler l'art. 18 AP comme suit : « Le service octroie aux fournisseurs de services de télécommunication un certificat attestant qu'ils sont *en principe capables* d'exécuter les surveillances *prévues dans le cadre de la présente loi*. *En particulier, il octroie aux fournisseurs de services de télécommunication tenus d'exécuter des surveillances un certificat attestant qu'ils disposent d'interfaces compatibles avec le système de traitement de la Confédération*. Le service fixe les modalités de la certification. » Afin que le principe de la proportionnalité soit respecté, Verizon propose en outre que les fournisseurs de services de télécommunication aient, dans certains cas, la possibilité de recourir à un tiers sans que cela implique forcément pour ce dernier l'obligation de se faire certifier. Les participants susmentionnés s'opposent à ce que les fournisseurs de services de télécommunication devant exécuter des surveillances prennent à leur charge les frais qui en résultent. HR est également contre et souligne l'importance que cette réglementation revêt du point de vue de la politique industrielle : depuis quelques années, Internet a été en Suisse un vivier de start-up dynamiques qui ont créé de nombreux emplois porteurs d'avenir. A noter également que plusieurs entreprises d'envergure se sont installées en Suisse au cours de ces dernières années, comme Google à Zurich. Le calcul particulièrement difficile des frais et le coût élevé de la certification constituent des obstacles importants à l'accès au marché qui réduisent les chances de réussite des start-up et l'attrait des implantations internationales. CCC, INT et PPS considèrent, pour leur part, que la prise en charge des frais liés à une certification par les fournisseurs de services Internet serait disproportionnée. Cablecom souligne que, dans toute autre relation commerciale, les frais liés aux tests d'intégration des interfaces techniques sont pris en charge par le mandataire, autrement dit, chacun prend en charge ses propres frais. Il ne comprend pas que le service puisse employer des personnes pour l'aider lors des certifications mais que ces dernières soient payées par les fournisseurs de services de télécommunication. Voilà pourquoi il s'oppose à ce que ces derniers prennent totalement en charge les frais liés à ces certifications et demande la suppression des art. 18 et 24 AP. Selon SIUG, une branche entière de l'économie est contrainte de se « mettre en condition » et de mener des enquêtes pénales pour l'Etat de façon indépendante. Les fournisseurs qui

---

82 LU, NW, BL, SG, AG, GL, GR, TG, JU, CCDJP, CAPS, FSFP, CP.

83 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.

n’ont pas de certificat et qui doivent exécuter une surveillance doivent prendre en charge des frais inattendus, ce qui peut avoir de graves conséquences financières pour certains d’entre eux. Il se peut aussi que les fournisseurs qui se font certifier n’aient jamais à exécuter de surveillance. Dans ce cas, non seulement, ils auront perdu du temps et de l’argent, mais, en plus, ils n’auront pas contribué à ce qu’on gagne en efficacité dans la poursuite des infractions. SIUG propose également de biffer les art. 18 et 24 AP.

(IT)19, SWICO, hp et COG préconisent que le but de la certification et la procédure en la matière soient définis plus clairement. De plus, ils souhaitent que l’art. 18 AP énumère les personnes devant se faire certifier. Selon SWICO, hp et COG, les frais liés à une certification doivent, en outre, être pris en charge par le service.

JDS et droitsfondamentaux.ch se déclarent favorables à une suppression des art. 18 et 24 AP car ils estiment que ces derniers font disparaître la liberté de pouvoir proposer des formes modernes de communication au profit d’un système de contrôle et d’autorisation étatique.

switch et switchplus s’opposent, eux aussi, à une obligation de fait de se faire certifier. Selon eux, il convient de mentionner clairement que les personnes entrant dans le champ d’application de la LSCPT doivent se soumettre à un test de conformité et qu’elles sont exemptées de la certification si celui-ci s’avère concluant. Dans le cas contraire, il y aura lieu d’harmoniser les exigences relatives à la certification avec celles prévues par les directives concernant l’« acceptance testing » pour éviter que les moyens doivent être mis en œuvre à double.

ISSS relève que le but de la certification et la procédure en la matière sont décrits de manière très imprécise et se pose la question essentielle suivante : l’aptitude d’un fournisseur à exécuter des surveillances en conformité avec la loi peut-elle être déterminée dans le cadre d'une procédure de certification ? La disposition en cause ne fait, par ailleurs, pas ressortir clairement si les fournisseurs de services Internet et les personnes visées par l'art. 2, al. 1, let. b, AP doivent se faire certifier.

4. Obligations dans le domaine de la surveillance de la correspondance par poste

4.1. Art. 19

[1] Dans la mesure où l’ordre de surveillance le prescrit, les personnes qui exécutent des surveillances de la correspondance par poste en vertu de la présente loi sont tenues de livrer à l’autorité qui a ordonné la surveillance les envois postaux et les données indiquant quand et avec quelles personnes la personne surveillée a été ou est en liaison par poste et les données relatives au trafic et à la facturation. A la demande de l'autorité qui a ordonné la surveillance, elles lui fournissent des renseignements complémentaires sur la correspondance par poste des personnes concernées.

[2] Elles doivent conserver douze mois les données mentionnées à l’al. 1.

4.1.1 al. 1

Selon plusieurs participants[84], cette disposition ne fait pas ressortir clairement qu'il faut s'assurer, dans le cadre de la surveillance de la correspondance par poste, que non seulement le fournisseur livre les envois postaux à l'autorité qui a ordonné la surveillance mais aussi qu'il les récupère dans les plus brefs délais une fois qu'ils ont été contrôlés par la police et qu'il les achemine vers leur destinataire. Ces participants demandent que la loi soit précisée dans ce sens.

La Poste Suisse souligne que l'enregistrement des données relatives au trafic des envois est lacunaire, raison pour laquelle il n'est pas possible de fournir rétroactivement des informations sur le contenu ou les données secondaires de tous les envois. Les envois déposés dans une boîte aux lettres ou dans un office de poste ainsi que tous les autres envois (lettres) non recommandés ne sont répertoriés dans aucun des systèmes de transport ou de traitement de la Poste Suisse, ce qui explique qu'aucune donnée secondaire relative à ces derniers ne peut être consultée ni communiquée rétroactivement. Il en va autrement pour les lettres et les colis envoyés en recommandé et les envois que l'on peut suivre grâce au « système Track & Trace » de la Poste Suisse. Cette dernière peut, en effet, fournir des renseignements à leur sujet dans la mesure de ce qui a été fait jusqu'à présent. Elle relève que la révision de la LSCPT ne crée aucune nouvelle possibilité ni obligation pour elle.

PES, JDS et droitsfondamentaux.ch trouvent absurde de parler de données secondaires dans le cadre de la surveillance de la correspondance par poste. Ils indiquent que le nombre de surveillances de la correspondance par poste a diminué plus vite que n'a augmenté le nombre de formes électroniques de communication et demandent qu'au lieu de multiplier par deux la durée de conservation des données, on supprime cette disposition et on mette fin à la pratique que cette dernière institue. JDS met en avant la quantité considérable de données qui s'accumulent et qui n'ont que peu d'importance pour la poursuite des infractions. Selon JDS et droitsfondamentaux.ch, on ne peut garantir l'exactitude des renseignements concernant l'expéditeur - si tant est qu'ils soient fournis -, à moins de demander une pièce d'identité à toute personne venant faire un dépôt dans un office de poste. Eu égard aux conséquences qu'aurait une application à la lettre, SIUG et Swiss Privacy Foundation trouvent également cette disposition insuffisante.

4.1.2 al. 2

Un grand nombre de participants[85] se félicite expressément de l'allongement de six à douze mois du délai de conservation des données permettant l'identification des usagers. Parmi eux, onze[86] demandent s'il ne serait pas possible d'allonger davantage ce délai dans la mesure où les données sont généralement conservées pendant dix ans par les fournisseurs. Pour SZ, l'allongement du délai de conservation des données n'est envisageable que si des mesures législatives visant à garantir la sécurité des données ainsi que la transparence de leur communication et à prévenir toute utilisation abusive sont prises.

L'allongement à douze mois du délai de conservation des données secondaires dans le domaine de la correspondance par poste ne pose aucun problème à la Poste Suisse.

Cablecom et SKS sont, quant à eux, contre l'allongement du délai de conservation des données. SKS fait valoir que la correspondance par poste ne cesse de diminuer au profit de la

---

84 ZH, LU, NW, GL, GR, TG, VS, JU, CCDJP, CAPS.
85 ZH, LU, NW, GL, GR, TG, VS, JU, SZ, UR, OW, FR, SO, AG, GE, CCDJP, CAPS.
86 ZH, LU, NW, GL, GR, TG, VS, JU, SZ, CCDJP, CAPS.

correspondance électronique et que les données recueillies n'ont presque aucune utilité pratique pour la poursuite des infractions.

5. Obligations dans le domaine de la surveillance de la correspondance par télécommunication

Plusieurs participants appartenant à la branche des télécommunications[87] proposent que la section 5 soit rebaptisée comme suit : « Obligations des fournisseurs de services de télécommunication ». Ils justifient leur proposition par le fait que l'art. 20 AP relatif aux renseignements sur les raccordements de télécommunication ne fait nullement référence à une surveillance ou à une violation du secret des télécommunications.

Swisscom demande que trois catégories de prestations, à savoir renseignements sur les raccordements, surveillances en temps réel et conservation des données permettant l'identification des usagers, soient définies dans la section 5 et que des règles claires soient fixées pour chacune d'entre elles . De plus, les dispositions en question doivent être coordonnées avec le CPP. Ce dernier établit, en effet, clairement que seule la surveillance de certains raccordements, utilisés par des personnes suspectes, doit être autorisée. La recherche à tâtons d'éléments suspects est donc interdite. Cette coordination permettrait, selon Swisscom, d'éviter que des surveillances soient – comme c'était le cas jusqu'à présent – ordonnées alors qu'elles sont illicites d'après le nouveau CPP.

5.1. Art. 20 Renseignements sur les raccordements de télécommunication

[1] Les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi fournissent au service les données suivantes sur des raccordements déterminés:

a. le nom, le prénom, la date de naissance, l'adresse et, si celle-ci est connue, la profession de l'usager;

b. les ressources d'adressage définies à l'art. 3, let. f, de la loi du 30 avril 1997 sur les télécommunications ;

c. les types de raccordements.

[2] Les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi doivent être en mesure de fournir durant au moins deux ans après l'ouverture d'une relation commerciale dans le domaine de la téléphonie mobile et d'Internet avec leurs clients n'ayant pas souscrit d'abonnement les renseignements relatifs à cette relation prévus à l'al. 1.

[3] Si un acte punissable est commis par Internet, les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi doivent fournir au service toute indication permettant d'identifier son auteur.

[4] Le Conseil fédéral règle la forme des demandes et leur conservation. Il peut autoriser l'accès aux répertoires existants et non accessibles au public aux autorités mentionnées à l'art. 14. Il peut également rendre ces données accessibles au service par une consultation en ligne. Il peut prévoir que la communication des données soit exécutée gratuitement et à n'importe quel moment.

IT(19), SWICO, hp et COG demandent la mise en place d'un organe externe qui surveillerait et contrôlerait le service à tout instant. SWICO, hp et COG estiment en effet que le fait de pouvoir accéder à toutes les données de communication, tel que le prévoit l'AP, et donc d'avoir la garantie de pouvoir identifier les usagers, donne aux autorités fédérales des possibilités de surveillance étendues.

5.1.1 al. 1

[87] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

UNISG et UNIZH entendent que les « raccordements dans Internet », qui doivent être considérés comme des raccordements de télécommunication selon le rapport explicatif, soient explicitement mentionnés. switch et switchplus relèvent que la notion de « raccordement de télécommunication » n'est définie ni dans l'OSCPT ni dans la LTC. Il n'en est question que dans l'annexe 1.7 à l'ordonnance de l'Office fédéral de la communication du 9 décembre 1997 sur les services de télécommunication et les ressources d'adressage[88]. Dans celle-ci, on entend par « raccordement de télécommunication » la téléphonie par GSM[89]/UMTS[90], PSTN[91]/ISDN[92] et IP (VoIP). Ceux qui proposent des services de VoIP publics sont tenus de fournir les données mentionnées à l'al. 1, contrairement à ceux qui en proposent des privés.

let. a

Dix participants[93] se félicitent expressément que l'on puisse dorénavant également demander la date de naissance. ZH, LU, CCPCS et BL souhaitent par ailleurs qu'on saisisse le type et le numéro de la pièce d'identité afin de garantir l'identification des clients, notamment des clients de téléphonie mobile utilisant des cartes à prépaiement. BL évoque des cas d'abus dans lesquels des relations commerciales auraient été ouvertes sur la base de fausses coordonnées et où un employé aurait, après avoir enregistré correctement une carte SIM prépayée, enregistré d'autres cartes SIM au nom du client.

D'autres participants[94] préconisent, au contraire, qu'on supprime l'obligation de demander la date de naissance.

UNISG et UNIZH attirent l'attention sur le fait que les usagers utilisant, p. ex., un terminal d'accès à Internet public ne peuvent pas être identifiés.

Selon HR, la let. a aurait pour effet que les adresses e-mail ne peuvent plus être attribuées de façon anonyme. Ce participant se demande si les fournisseurs de services à valeur ajoutée qui ne fournissent pas d'adresse personnelle doivent garantir la corrélation entre l'adresse e-mail et la personne physique ou s'ils peuvent renvoyer au titulaire d'un nom de domaine conformément au protocole Whois. Il se pose, par ailleurs, la question suivante : n'est-il pas punissable d'autoriser une personne à s'inscrire à un forum ou à un blog sans lui demander sa date de naissance ?

let. b

Neuf participants[95] demandent que la let. b soit reformulée comme suit : « les ressources d'adressage définies à l'art. 3, let. f *et g*, de la loi du 30 avril 1997 sur les télécommunications. » Pour justifier leur demande, ils relèvent que seuls les appareils de téléphonie mobile sont mentionnés aux art. 270ter et 274, al. 4, let. d, CPP. Les ordinateurs portables et les notebooks munis de cartes SIM pour la transmission par réseau de téléphonie mobile ne sont donc pas concernés.

VD souhaite des précisions dans la loi en ce qui concerne l'identification des adresses IP. Selon la pratique actuelle, la demande portant sur un tel objet est considérée comme une

---

88 RS 784.101.113/1.7
89 Global System for Mobile Communications.
90 Universal Mobile Telecommunications System.
91 Public Switched Telephone Network.
92 Integrated Services Digital Network.
93 ZH, LU, SO, GL, GR, TG, VS, JU, CCDJP, CCPCS.
94 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
95 ZH, LU, GL, GR, TG, VS, JU, CCDJP, CCPCS.

simple mesure fondée sur l'art. 14 LSCPT, ce qui permet aux services de police d'obtenir les données sans passer par l'autorisation d'un magistrat. Or, selon VD, l'AP ne permet pas d'admettre d'emblée le maintien de cette pratique. Il demande donc qu'il soit clairement précisé que l'accès à l'adresse IP comme au numéro de téléphone n'est pas subordonné à l'obtention d'une autorisation au sens de la loi mais peut avoir lieu, comme à l'heure actuelle, par la voie simplifiée.

let. c

Pas de remarques.

5.1.2 al. 2

BL estime que la réglementation relative à la durée de l'obligation de renseigner qui est prévue par l'AP n'est pas claire. Il ne voit, en particulier, pas pourquoi ce délai a été fixé à deux ans sans tenir compte du fait que la relation commerciale pouvait encore être active à ce moment-là. Un fournisseur de services de télécommunication doit être en mesure de fournir les renseignements prévus à l'al. 1 pour toute relation commerciale active. BL propose donc que cette disposition soit reformulée comme suit : « (…) *pendant deux ans au maximum après fermeture de la relation commerciale ou désactivation du raccordement* (…) ». Il y a en outre lieu de compléter l'art. 20, al. 2, AP en ajoutant que les fournisseurs de services de télécommunication doivent être en mesure, durant le délai prévu, de fournir une copie des pièces d'identité de leurs clients. VD demande par ailleurs que les cartes « wireless » à prépaiement soient explicitement mentionnées.

Huit participants[96] proposent le nouveau libellé suivant : « Les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi doivent être en mesure de fournir durant au moins deux ans après l'ouverture d'une relation commerciale dans le domaine de la téléphonie mobile avec leurs clients n'ayant pas souscrit d'abonnement et *s'étant vu remettre les cartes* les renseignements relatifs à cette relation prévus à l'al. 1 ». L'expression « et d'Internet » doit être biffée car il est impossible de soumettre, p. ex., l'utilisation de cartes « wireless » à prépaiement à un enregistrement obligatoire.

UNIZH demande que le délai de deux ans qui est proposé soit ramené à douze mois, soit le délai général de conservation prévu par l'art. 19, al. 2, AP et l'art. 23 AP, à défaut de quoi une procédure coûteuse sera nécessaire si l'on veut faire le tri entre des données ayant des délais de conservation différents.

5.1.3 al. 3

Pour SO, le fait que l'obligation de fournir au service toute indication permettant d'identifier l'auteur d'une infraction est étendu aux personnes visées par l'art. 2, al. 1, let. b, AP, permettra d'alléger considérablement le travail de la police.

UVS souhaite des précisions en ce qui concerne les renseignements sur les raccordements de télécommunication. Selon elle, les données que les fournisseurs de raccordements Wi-Fi publics doivent collecter et conserver ne sont pas définies de manière suffisamment claire.

---

[96] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

Huit participants[97] proposent le nouveau libellé suivant : « Si un acte punissable est commis par Internet, les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi doivent fournir au service *toutes les indications sur les raccordements de télécommunication dont ils disposent et qui sont propres à permettre l'identification de l'auteur*. » Ils justifient leur proposition en invoquant que seuls des renseignements sur les raccordements doivent être fournis et non des données de communication. De plus, on ne peut exiger des données autres que celles prévues par l'al. 1 que si elles sont disponibles. L'identification de l'auteur d'un acte punissable peut être un objectif et non une obligation contraignante. Cablecom indique qu'il est la plupart du temps possible d'identifier l'appareil avec lequel l'acte punissable a été commis mais que c'est impossible quand l'appareil-cible est raccordé au réseau par le bais d'un « routeur » privé. Dans ce cas, on peut seulement identifier le routeur et non le terminal utilisé. Dans ce contexte, UNIZH fait remarquer qu'il convient de faire une distinction entre l'abonné et la personne à surveiller. Seules des données relatives à l'abonnement souscrit pour l'utilisation du raccordement câblé ou à la personne pour laquelle une ressource d'adressage a été réservée sont disponibles. Déterminer qui a effectivement utilisé un ordinateur ou un smartphone relève presque de l'impossible. C'est la raison pour laquelle Cablecom propose le libellé suivant : « permettant d'identifier son auteur *dans la mesure où elle concerne un raccordement de télécommunication* ».

Selon switch et switchplus, il semble que l'al. 3 ne s'applique pas seulement aux raccordements de télécommunication. Ils demandent donc que soit spécifié dans la disposition en cause que seul ce type de raccordements est visé et non les noms de domaines.

ISSS demande que l'objet et l'étendue de l'identification des utilisateurs soient adaptés et concrétisés compte tenu des formes actuelles et futures d'utilisation de la communication numérique et d'Internet. Soumettre les fournisseurs de services de télécommunication à l'obligation d'identifier toutes les personnes prenant part à un échange de communications numériques ou utilisant Internet placerait ces derniers face à des difficultés quasiment insurmontables.

Aux yeux de KFG, cette disposition constitue un pas vers une surveillance totale d'Internet. Chaque utilisateur doit s'identifier. Il demande que la disposition soit modifiée de telle sorte que seules les personnes utilisant un raccordement à Internet qui se sont enregistrées doivent être identifiées ou, à défaut, qu'elle soit purement et simplement biffée.

ifpi et safe attirent l'attention sur le fait que les droits privés constituent le bien juridique protégé par les dispositions pénales réprimant les violations du droit de la propriété intellectuelle. L'ordre juridique d'Internet tout entier s'en trouverait bouleversé si l'on retirait à l'ayant droit la possibilité de régler son contentieux directement avec celui qui a enfreint la loi. Il serait alors contraint d'engager une poursuite pénale. Cette criminalisation indésirable des particuliers qui enfreignent la loi n'est pas indispensable si les ayants droit connaissent les coupables et qu'ils veulent passer par une procédure civile. ifpi et safe demandent donc que l'AP soit modifié de sorte que les indications mentionnées à l'al. 3 soient fournies sur demande à la victime ou que cette dernière puisse les obtenir directement du fournisseur de services Internet si elle établit qu'une personne utilisant une adresse IP a, selon toute vraisemblance, enfreint la loi.

5.1.4 al. 4

[97] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

Invoquant la ratification de la convention sur la cybercriminalité[98], quelques participants[99] critiquent le fait que cet alinéa soit formulé de manière potestative. Ils demandent que l'obligation de communiquer des données gratuitement et à tout moment soit inscrite dans la loi.
SZ, NW, SG et CAPS souhaitent que les autorités de poursuite pénale puissent consulter les données en ligne. Selon les fournisseurs, il faut aujourd'hui parfois attendre plusieurs heures avant de savoir à qui appartient un numéro de téléphone, ce qui, lors de recherches dans des cas d'urgence ou en cas d'infraction grave, n'est pas tolérable. Les fournisseurs refusent de mettre en ligne ces données car ils craignent que leurs concurrents ne s'en servent ; mais ce problème est techniquement facile à résoudre.

Des participants appartenant à la branche des télécommunications[100] déplorent qu'on en demande toujours plus aux fournisseurs de services de télécommunication. Aussi exigent-ils que la dernière phrase de l'al. 4 soit biffée.

Pour Cablecom, la notion de « consultation en ligne » qui est utilisée à l'al. 4 n'est pas très claire.

UNISG et UNIZH estiment que la possibilité qui est offerte aux autorités d'accéder aux répertoires existants et non accessibles au public, est problématique.

switch et switchplus veulent que l'accès aux répertoires prévu par cette disposition se limite expressément à ceux qui concernent des raccordements de télécommunication.

5.2. Art. 21 Obligations lors de l'exécution de surveillances

[1] Les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi doivent fournir au service, lorsque celui-ci le demande, les communications de la personne surveillée ainsi que les données indiquant quand et avec quels raccordements la personne surveillée a été ou est en liaison par télécommunication et les données relatives au trafic et à la facturation. L'art. 16, let. d est réservé. Ils sont également tenus de fournir les informations nécessaires à la mise en œuvre de la surveillance.

[2] Les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi transmettent dans les meilleurs délais les données indiquant quand et avec quels raccordements la personne surveillée a été ou est en liaison par télécommunication et les données relatives au trafic et à la facturation et, si possible en temps réel, les communications de la personne surveillée. Elles suppriment les chiffrements qu'elles ont opérés.

[3] Les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi transmettent au service tout le flux de données concernant la personne surveillée. A la demande du service, elles sont tenues de ne lui transmettre que le type ou les types de données désignés composant le flux de données considéré.

[4] Les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi prêtent au service le concours nécessaire à la mise en œuvre d'une mesure de surveillance impliquant de devoir recourir à des programmes informatiques dans le but de permettre l'interception et la lecture des données (art. 270bis CPP et art. 70a^{bis} de la procédure pénale militaire).

[5] Toutes les personnes exécutant des surveillances de la correspondance par télécommunication en vertu de la présente loi qui participent à l'exploitation du service de télécommunication à surveiller sont tenues de fournir les données en leur possession à celle parmi celles-ci chargée de la surveillance.

De nombreux participants[101] considèrent que les obligations concrètes ne sont pas réglées

98 FF **2010** 4275
99 ZH, LU, GL, GR, TG, VS, JU, CCPCS, CCDJP.
100 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.
101 PDC, PLR, UDC, GPS, SKS, economiesuisse, ICT, ePower, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, SIUG, SPICT.

avec une clarté suffisante. Aussi, par souci d'assurer la sécurité du droit, requièrent-ils l'élaboration d'un cahier des charges précis, certains formulant des propositions de normes à cette fin. Swisscom exige en outre que les fournisseurs de services de télécommunication ne soient pas tenus d'assumer les tâches de coordination pour l'ensemble des services offerts par des tiers. Ils estiment que ces tiers doivent être directement soumis aux instructions du service.

5.2.1 al. 1

CCPCS préconise que l'on étende l'obligation de communiquer les informations à tous les cas dans lesquels la personne surveillée s'est limitée à établir une communication. Plusieurs participants de la branche des télécommunications[102] proposent sous la forme de normes rédigées d'instaurer une restriction selon laquelle l'obligation de surveillance s'appliquerait au trafic via un raccordement déterminé qui a été fourni par un opérateur en matière de télécommunication. Par ailleurs, ils préconisent l'adoption d'un article distinct concernant le relevé de données permettant l'identification des utilisateurs. Cablecom se demande ce qu'il faut entendre exactement par « informations nécessaires ».

5.2.2 al. 2

Par voie de conséquence, les mêmes participants[103] requièrent que l'obligation de surveillance soit, comme à l'al. 1, limitée à un raccordement déterminé qui a été fourni par un opérateur en matière de télécommunication. Enfin, ils demandent que l'on précise que la lisibilité des données fournies ne peut être garantie.

Un nombre non négligeable de participants[104] demande que l'on biffe les expressions « dans les meilleurs délais » et « si possible en temps réel », estimant qu'elles sont à la fois imprécises et inacceptables compte tenu des coûts d'infrastructure importants auxquels il faut s'attendre. Si CCPCS considère également comme trop imprécise la formule « dans les meilleurs délais », elle demande en revanche que l'on introduise dans la loi une référence aux directives techniques qui fixeront le délai dans lequel les données seront fournies.

UNISG et UNIZH mettent en doute la faisabilité technique de la suppression des chiffrements telle qu'elle est prévue. IT(19), SWICO, hp et COG exigent l'adoption d'une norme légale obligeant les fournisseurs de services de télécommunication à informer leurs clients faisant l'objet d'une mesure de surveillance avant que cette mesure ne soit appliquée, que le chiffrement opéré peut être supprimé dans le cadre d'une mesure de surveillance au sens de la LSCPT et que le client peut, par la suite, être l'objet d'une telle mesure. De même, ISSS part du principe qu'en vertu du devoir de fidélité et de diligence que la loi impose au fournisseur, celui-ci est tenu d'informer le client que le chiffrement utilisé est susceptible d'être supprimé. Elle exige, d'une part, que la divulgation du chiffrement opéré par les fournisseurs de services de télécommunications soit limitée aux cas clairement définis par la loi et, d'autre part, que l'on prévoie une procédure permettant à ces fournisseurs de faire valoir les intérêts qu'ont leurs clients à ce que leurs communications soient protégées et, au besoin, de saisir le juge pour les défendre.

HR relève que le libellé est abstrus et demande que l'on précise que le chiffrement n'est pas frappé d'une interdiction générale. Il estime que le cryptage de bout en bout constitue un

---

[102] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
[103] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
[104] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom, IT(19), ISSS, PPS.

avantage non négligeable pour l'activité des ONG[105] (par exemple, le CICR ou Amnesty International).

5.2.3 al. 3

Onze participants[106] estiment qu'il est techniquement impossible de trier des données bien déterminées dans le flux des informations à transmettre. Ils préconisent donc la suppression de la disposition correspondante (v. aussi supra, partie III. ch. 3.3.6, remarques concernant l'art. 16, let. f, AP). UNIZH met, pour le moins, en doute la faisabilité technique d'un tel tri. Quelques participants[107] exigent que le filtrage du flot de données incombe au service.

privatim, estimant que le libellé de la disposition est trop large, propose la formulation restrictive suivante: …. « tout le flux de données *découlant de l'ordre de surveillance ».* A défaut de cette formulation, on porterait - de l'avis de ce participant - atteinte non seulement au principe de précision, mais encore à ceux de la finalité et de la proportionnalité.
CP relève que la sélection de données déterminées oblige à consulter des données hautement sensibles et recèle un risque de perte de données. A son sens, il faut donc remanier la disposition en cause. SIMSA estime que l'expression « flux de données » ne permet pas de limiter l'ampleur de la surveillance et, partant, porte atteinte au principe selon lequel on doit utiliser les données personnelles de manière confidentielle. Seules les données relevant des communications personnelles de la personne surveillée sont pertinentes du point de vue de la surveillance. IT(19), SWICO, hp et COG comparent la surveillance de tout le flux de données à une perquisition. Une telle mesure de surveillance ne peut être appliquée qu'avec l'autorisation du juge, qui doit être préalablement produite au fournisseur de services de télécommunication et aux fournisseurs de services Internet. Ces participants demandent, en outre, que le travail occasionné par le tri des données soit rétribué.

ISSS met en garde contre le développement de systèmes de filtrage et de tri, estimant qu'ils peuvent aussi, malheureusement, avoir pour effet de faciliter aux tiers non autorisés la recherche de fichiers et de flux de données, ce qui fait baisser le niveau de la sécurité de l'information dans notre pays. Aussi, ce participant préconise-t-il que des programmes d'analyse et de filtrage ne soient exécutés que dans des cas qualifiés, en vertu d'une ordonnance du juge.

5.2.4 al. 4

On trouvera dans la partie III, chiffre 11.1.2 ad art. 270bis CPP des remarques générales concernant les fins nouvelles auxquelles il est prévu de recourir à des programmes informatiques. Quant aux observations formulées à propos du concours, au sens large, que se doivent de prêter les personnes qui exécutent des surveillances, elles peuvent être récapitulées comme suit :

Plusieurs participants[108] déplorent que le libellé ne fasse pas ressortir clairement qui est compétent pour mettre au point, acquérir et utiliser de tels programmes. Cela étant, privatim, SIMSA et ISSS demandent que la notion de « concours nécessaire » soit précisée.

D'autres participants[109] estiment que l'utilisation de tels programmes ne doit pas être déléguée à des entreprises du secteur privé mais demeurer de la compétence exclusive de

---

105 Organisations non gouvernementales.
106 UDC, GPS, SKS, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
107 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
108 ZH, BL, ZG, LU, SP, privatim, ISSS.

l'autorité. Au regard du système juridique suisse, il n'est pas souhaitable que des entreprises privées soient contraintes de s'impliquer dans des opérations de police. Aux yeux du PPS, cette remarque doit aussi impérativement s'appliquer à la fabrication et à la maintenance des systèmes d'infiltration.

D'autres participants[110] sont de l'avis que, d'une manière générale, on ne saurait raisonnablement exiger d'une entreprise privée qu'elle installe sur les instructions du service des « Government Software » (souvent aussi appelés « chevaux de Troie ») dans le système informatique de ses clients. Non seulement une telle implication forcée dans des opérations de police est singulière, mais encore elle est de nature à saper la confiance qui doit régner entre les fournisseurs de services et leurs clients puisque le recours à de tels programmes va carrément à l'encontre de leurs intérêts. Ces participants qui refusent absolument d'être soumis à une quelconque obligation de prêter leur concours à de telles pratiques, demandent - conjointement avec IT(19) et Cablecom - la suppression de l'al. 4.

RD relève que ces programmes qui sont, en eux-mêmes, source de problèmes, sont très controversés. Il estime que l'on va trop loin en voulant contraindre, sans cautèles et sans aucune nécessité, les fournisseurs de service à prêter leur concours aux autorités sous une forme ou sous une autre pour le piratage de systèmes appartenant à des clients ou à des tiers. En agissant ainsi, les pouvoirs publics ébranlent fortement la confiance placée dans une branche complète de l'industrie et font peser sur la sécurité des risques qui, en définitive, sont nuisibles à l'ensemble de l'économie.

switch souligne qu'en sa qualité d'entreprise exploitant des réseaux, elle met en œuvre des mesures de large ampleur pour lutter contre les virus et les logiciels espions, de sorte qu'au cas où une mesure de surveillance devrait être exécutée, elle serait dans l'incapacité de distinguer un virus transmis involontairement d'un logiciel espion. Aussi, une collaboration avec le service est-elle impérative. En outre, l'instauration d'une telle mesure de surveillance exigerait la suspension de toutes les mesures de lutte contre les virus. Switch appelle de ses vœux un libellé plus rigoureux permettant d'éviter ce conflit d'objectifs.

5.2.5 al. 5

VD demande que cette disposition soit formulée de manière plus précise. D'autres participants[111] souhaitent qu'elle soit purement et simplement biffée.

5.3. Art. 22 Identification des utilisateurs qui accèdent à Internet

Les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi doivent prendre les mesures techniques nécessaires permettant d'identifier les utilisateurs qui accèdent à Internet par leur entremise.

Un nombre relativement important de participants[112] se félicite expressément de cette disposition. Selon ZH, l'identification des utilisateurs d'Internet permet de recueillir des indices importants voire décisifs pour la poursuite pénale. Par ailleurs, la possibilité d'identifier les internautes peut avoir un effet préventif. SZ et CAPS rappellent la situation existant dans certains pays voisins, où il n'est pas toujours possible d'avoir accès à Internet sous le couvert de l'anonymat et sans déclarer son identité. Ces deux participants estiment que la charge

---

109 UDC, PDC, PLR, PPS, economiesuisse, Swisscable.
110 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SWICO, hp, COG.
111 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.
112 ZH, LU, SZ, NW, SO, GL, GR, TG, VS, JU, CCDJP, CCPCS, CAPS.

administrative occasionnée aux fournisseurs de service par les accès temporaires à Internet (utilisation des systèmes mis à la disposition de la clientèle par les hôtels, connexion via les cybercafés, etc.) est raisonnable.
En revanche, un grand nombre de participants[113] proposent que l'on supprime ou, du moins, modifie cette disposition. VD, ISSS et PES estiment que l'obligation qu'elle statue est disproportionnée, notamment en ce qui concerne l'accès sans fil à Internet au moyen du« Wi-Fi » (points d'accès dans les gares, les écoles, les hôtels, etc.). Elle conduirait à la suppression des liaisons Internet qui sont aujourd'hui mises à la disposition du public. Ces participants demandent donc sinon la suppression, du moins une profonde adaptation de cette obligation qui serait unique en Europe. UDC dénonce la charge disproportionnée qu'engendrerait une telle obligation et demande, elle aussi, sa suppression. Pour leur part, UVS et privatim rejettent la disposition proposée notamment aux motifs qu'elle serait facile à éluder (« Proxies »; possibilité de masquer l'adresse IP, connexion au moyen d'une carte SIM de deuxième main) et qu'elle restreindrait de manière excessive la liberté personnelle de l'ensemble des utilisateurs d'Internet. Selon JDS et droitsfondamentaux.ch, la disposition en question est absurde et révélatrice de l'approche totalitaire qui a été suivie par les auteurs du projet. Ainsi, pour pouvoir téléphoner d'une cabine publique point n'est besoin d'établir préalablement son identité. La disposition proposée aurait, par exemple, pour effet d'obliger la personne qui prête son ordinateur ou son smart phone à une connaissance pour qu'elle surfe sur la toile à contacter préalablement son fournisseur de services pour lui permettre l'identification de cet utilisateur. Autre conséquence de cette disposition: les fournisseurs de services seraient contraints d'interdire à leurs clients d'utiliser des réseaux dont l'accès n'est pas protégé par un mot de passe. Par ailleurs, l'identification par le biais d'un téléphone portable, telle que proposée, serait exclue pour un certain nombre de personnes tout en état facile à éluder. RD estime aussi que cette disposition n'a aucun sens. A l'appui de cet avis, il rappelle également que les utilisateurs du téléphone n'ont pas besoin d'établir leur identité. Les participants sont relativement nombreux[114] à relever que si un fournisseur de services de télécommunication est en mesure d'identifier ses abonnés (avec lesquels il est lié par contrat), il est, en revanche, dans l'incapacité d'identifier chacun des utilisateurs qui se connecte à Internet via un raccordement. Ces participants sont de l'avis qu'il faut biffer la disposition. Selon IT(19), il y a lieu de déterminer clairement le temps maximum qui peut être consacré à une identification et de rémunérer le travail correspondant. Cablecom, switch et switchplus plaident également en faveur d'une suppression ou d'une reformulation de la disposition, soulignant que l'identification de l'appareil utilisé ne peut être réalisée qu'une seule fois, au maximum. Toutefois, cette identification n'est possible que si tous les appareils interposés (routeur, points d'accès sans fils, etc.) sont placés sous la responsabilité et le contrôle technique de la personne chargée d'exécuter les mesures nécessaires à l'identification. L'identification par le biais d'un numéro de téléphone portable n'est pas viable: lorsque l'utilisateur se sert d'un téléphone portable étranger, il faut demander ses données à l'opérateur étranger qui, en l'occurrence, n'est pas soumis au droit suisse. PLR, CP et FSA se demandent si l'on s'est suffisamment interrogé sur la praticabilité et les conséquences de la réglementation prévue. KFG et PSP proposent ou bien de restreindre l'ampleur de l'obligation d'identification ou bien de supprimer la disposition. Selon EPFZ, UNISG et UNIZH, le législateur semble partir de l'idée que les écoles, les hôtels, etc. passent par un fournisseur d'accès traditionnel pour obtenir leur accès à Internet. Si les universités attribuent elles-mêmes leurs adresses IP, elles n'offrent pas leurs services au public. Elles sont donc des fournisseurs d'accès. Toutefois, elles ne sont pas des fournisseurs de services Internet au sens de l'art. 2, let. a, OSCPT et ne sont donc pas soumises à l'art. 22 AP. Selon les hautes écoles susmentionnées, le libellé de

---

[113] VD, PES, UDC, PLR, ISSS, UVS,. Privatim, JDS, droitsfondamentaux.ch,RD, IT (19),Cablecom, switch et switch plus, CP, FSA, KFG, PPS, EPF, UNISG, UNIZH.

[114] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SWICO, hp, COG, IT(19).

l'art. 22 est susceptible de permettre une surveillance d'ensemble. Aussi doit-il être minutieusement réexaminé sous l'angle de la proportionnalité et précisé.

5.4. Art. 23 Conservation des données

Les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi sont tenues de conserver durant douze mois les données indiquant quand et avec quels raccordements la personne surveillée a été ou est en liaison par télécommunication et les données relatives au trafic et à la facturation.

Sur le principe, de nombreux participants[115] se félicitent de l'allongement du délai de conservation. FR estime toutefois nécessaire d'évaluer préalablement l'ampleur des tâches supplémentaires que cet allongement imposera aux cantons. SO insiste sur la nécessité de cet allongement eu égard notamment aux procédures d'entraide judiciaire qui ont tendance à avancer péniblement. BS souhaite, en outre, que l'on règle la manière de traiter les découvertes fortuites. AR, SZ et VD préconisent que l'on complète la disposition par des normes concernant la sécurité des données, la protection contre l'usage abusif de données et la transparence du transfert de données.

Un groupe relativement important de participants[116] propose que, par le biais de la réglementation prévue, on porte à dix ans le délai de conservation de manière à garantir la disponibilité d'éléments d'enquête probants même après plusieurs années. Certains de ces participants relèvent que les fournisseurs de services de télécommunication conservent d'ores et déjà de leur propre chef les données durant dix ans. Neuf participants[117] proposent de limiter le délai *d'appel* des données à six ou douze mois, nonobstant le délai de conservation de dix ans. BE souhaite également que le délai de conservation des données secondaires soit supérieur à douze mois.

En revanche, un grand nombre de participants[118] rejettent la disposition. JDS, droitsfondamentaux.ch, PES et SKS font remarquer que les autorités risquent de conserver systématiquement des données sur des personnes au-dessus de tout soupçon. PES et SKS estiment que cette pratique est d'autant moins compréhensible qu'à la fin de juin 2010 la Délégation des Commissions de gestion a émis des doutes quant à l'exactitude et à la pertinence des données enregistrées dans la banque ISIS. Plusieurs participants[119] attirent en outre l'attention sur les frais élevés qu'induira l'allongement du délai de conservation alors que toute indemnité est censée être supprimée.

Selon SIUG, la disposition en cause ne fait nullement mention de la localisation des antennes de téléphonie mobile, qui est aujourd'hui prescrite par l'OSCPT. Il propose que cette localisation – si tant est qu'elle soit encore prévue sous l'empire du nouveau droit – soit réglée au niveau de la loi. La surveillance rétroactive, étendue à l'ensemble du territoire et non liée à des soupçons touche tous les habitants de la Suisse. Elle viole donc le principe de la proportionnalité. Or, la conservation des données secondaires pendant douze mois permet d'établir un profil détaillé des communications et des déplacements de tous les habitants de la Suisse. En outre, la nécessité de doubler le délai de conservation n'est pas établie. Les

---

115 OW, ZH, LU, SZ, NW, BL, GL, GR, TG, VS, JU, FR, SO, BS, AR, AG, TI, VD, GE, PDC, PLR CCDJP CCPCS, VPSB, CAPS, SPICT.
116 ZH, LU, SZ, NW, BL, GL, GR, TG, VS, JU, PLR, CCDJP, CAPS.
117 NW, GL, GR, TG, VS, JU, PLR, CAPS, CCDJP.
118 BL, GPS, PS, SKS, USS, JDS, droitsfondamentaux.ch, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SIUG, ISSS, SWICO, hp, privatim, COG, 3D4X, PPS.
119 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SWICO, hp, COG, PPS.

différents types de surveillance, les données qui doivent être conservées et les notions utilisées souffrent d'une absence de définitions claires. ISSS s'oppose également à la disposition proposée. Elle préconise, toutefois, qu'à la rigueur, le texte de la loi soit modifié de telle sorte que le service puisse, dans le cas d'espèce, enjoindre à un fournisseur de services de conserver les données servant à l'identification, plus longtemps mais au maximum douze mois.

BL, PS, 3D4X et privatim exigent une réglementation nouvelle qui réponde aux critères établis par la Cour constitutionnelle allemande dans le cadre de l'arrêt concernant la conservation des données secondaires[120]. 3D4X se demande comment une petite entreprise du secteur IT fait pour se payer des instruments de surveillance alors qu'elle ne bénéficie d'aucune indemnité. Dans le même ordre d'idées, les entreprises regroupées sous le vocable IT(19) relèvent que l'allongement du délai de conservation induira une augmentation des coûts pour les personnes tenues d'assurer cette conservation.

Cablecom soulève une question: comment les fournisseurs de services Internet entendent-ils procéder pour assurer la conservation des données lorsqu'ils n'en ont aucune parce que les appareils échappent à leur influence ?

UVS estime qu'il ne ressort pas clairement de la disposition quelles données les fournisseurs de raccordements Wi-Fi publics doivent collecter et conserver.

Se référant au libellé de la disposition, EPFZ, UNISG und UNIZH relèvent qu'à leur sens l'obligation de conserver les données ne vaut pas pour les exploitants de réseaux de télécommunication internes et de centraux domestiques.

FSA déplore que l'allongement du délai de conservation n'ait pas été motivé.

switch et switchplus souhaitent que l'on précise le libellé de l'article 23 AP de manière à ce qu'il soit statué clairement que les personnes visées à l'art. 2, al. 2, AP sont aussi tenues de conserver les données relatives au trafic.

safe préconise que l'on intègre également dans la disposition la recherche de personnes *inconnues* qui sont à l'origine d'un trafic de données sur Internet. Il estime en effet que le libel-

---

[120] BVerfG, 1 BvR 256/08 du 2.3.2010, al.-n. (1 - 345); extraits essentiels des considérants: le fait que les fournisseurs privés de services conservent pendant six mois des données, par mesure de précaution et en l'absence de circonstances particulières - ainsi que le prévoit la Directive 2006/24/EG du Parlement européen et du Conseil du 15 mars 2006 (JO L 105 du 13 avril 2006, p. 54, ci-après « Directive 2006/24/CE ») - n'est pas purement et simplement incompatible avec l'art. 10 de la Loi fondamentale. Le respect du principe de la proportionnalité exige que le législateur, lorsqu'il règle une telle conservation des données, tienne équitablement compte des atteintes aux droits fondamentaux dont elle est la cause. Selon les considérants de l'arrêt, il y a lieu d'adopter des normes suffisamment exigeantes et précises qui règlent la sécurité des données, leur utilisation, leur transparence, sans oublier les voies de droit. (…) La recherche de données et leur utilisation directe ne sont conformes au principe de la proportionnalité que si elles servent à l'exécution de tâches éminemment importantes en matière de protection des biens juridiques. Pour que cette condition soit remplie dans le domaine des poursuites pénales, il faut qu'il existe des soupçons étayés par des faits précis qu'une grave infraction a été commise. (…) Une utilisation exclusivement indirecte des données par les fournisseurs de services de télécommunication dans le but de fournir des renseignements sur les titulaires d'adresses IP est admissible qu'il existe ou non une liste limitative d'infractions ou de biens juridiques protégés et qu'il s'agisse ou non d'écarter des dangers ou d'assumer des tâches de renseignement. En revanche, dans le cadre de la poursuite d'inobservations de prescriptions d'ordre, la fourniture de tels renseignements ne peut être autorisée que dans des cas expressément définis par la loi (…) (trad.).

lé est trop étroit puisqu'il n'englobe pas le cas, pourtant important, dans lequel on ne recherche pas les raccordements d'une personne connue ou surveillée mais d'une personne inconnue qui est à l'origine d'un trafic de données déterminé sur Internet.

5.5. Art. 24 Certification

Les remarques concernant la certification sont consignées dans la partie III, ch. 3.5 ad art. 18 AP.

5.6. Art. 25 Information sur les technologies et services

A la demande du service, les personnes qui exécutent des surveillances de la correspondance par télécommunication en vertu de la présente loi l'informent en tout temps de manière détaillée sur la nature et les caractéristiques de toute technologie ou de tout service qu'elles ont mis ou vont mettre sur le marché.

Neuf participants[121] estiment que les technologies et les services qui seront mis sur le marché relèvent du secret d'affaires. Il est donc exclu d'introduire dans la loi une norme obligeant les entreprises concernées à divulguer au service des informations sur ces innovations. Toutefois, de telles informations, lorsqu'elles émanent d'experts, doivent être indemnisées. ISSS souligne qu'outre le fait que cette disposition mettrait en péril le secret d'affaires et le secret de fabrication, les technologies en question sont en bonne partie aux mains d'entreprises étrangères. Cette disposition est donc de nature à causer de notables problèmes à l'économie suisse, puisqu'elle peut être à l'origine de mesures de rétorsion et aboutir à ce que les titulaires des droits sur ces technologies, par crainte de leur divulgation, n'utilisent plus en Suisse leurs techniques et procédés les plus récents, ce qui rendrait un mauvais service à la société de l'information propre à la Suisse. Cela étant, ISSS demande que l'on entreprenne les démarches en vue de conclure un accord international.

De surcroît, SIMSA souligne le risque que cette disposition présente pour la protection de l'innovation. IT(19), SWICO, hp et COG demandent que l'art. 25 soit complété par une disposition exemptant les fournisseurs de services de l'obligation de divulguer des secrets d'affaires et des secrets professionnels.

switch et switchplus demandent que l'on précise si les personnes visées à l'art. 2, al. 2, AP sont aussi soumises à l'obligation d'informer. Ils estiment que cette obligation induit des frais de formation des agents de la Confédération concernés, frais qui doivent être dûment compensés.

5.7. Art. 26 Exploitants de réseaux de télécommunication internes et de centraux domestiques et personnes visées à l'art. 2, al. 1, n'exerçant pas leur activité dans le domaine de la correspondance par télécommunication à titre professionnel

Les remarques concernant l'obligation de surveillance à laquelle sont soumises les personnes précitées sont consignées dans la partie III, ch. 1.2.3 ad art. 2, al. 2, AP.

6. Surveillance en dehors d'une procédure pénale

[121] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, ISSS, Cablecom.

6.1. Art. 27 Recherche dans un cas d'urgence

[1] En dehors d'une procédure pénale, l'autorité compétente peut ordonner une surveillance de la correspondance par télécommunication limitée à l'identification des usagers, aux données relatives au trafic et à la localisation pour retrouver une personne disparue. Elle peut si nécessaire consulter des données relatives à des tiers non impliqués.

[2] Une personne est réputée disparue lorsque:

a. la police a constaté qu'il était impossible de la localiser, et que

b. des indices sérieux donnent lieu de penser que sa santé ou sa vie sont gravement menacées.

6.1.1 al. 1

Un nombre relativement important de participants[122] propose une adjonction précisant que, dans des cas bien déterminés, l'autorité peut ordonner que l'on relève non seulement les données permettant l'identification des utilisateurs mais encore le contenu de conversations de manière à permettre de vérifier si la personne disparue a réellement utilisé le raccordement surveillé. Cette surveillance étant censée être soumise à autorisation, la protection de la personnalité des personnes concernées sera garantie dans une mesure appropriée. Pour sa part, VD plaide en faveur d'une procédure plus simple qui permette d'entamer la surveillance sans attendre l'autorisation du juge.

Plusieurs participants appartenant à la branche des télécommunications[123] demandent que la surveillance soit limitée à la localisation des appels**.** Ils s'opposent à la consultation de données relatives à des tiers non impliqués**.** De surcroît, Cablecom part de l'idée que la disposition ne vaut que pour la téléphonie mobile car, dans l'état actuel des choses, il est impossible de localiser les appels passés via Internet.

FSA ne comprend pas les raisons pour lesquelles on se propose de biffer l'art. 8, al. 5 de l'actuelle LSCPT. Elle demande que cet al. soit repris à titre de complément.

De l'avis de SIMSA, les fournisseurs de services peuvent à peine apprécier les effets de cette disposition, notamment en ce qui concerne les données relatives à des tiers non impliqués. SZ souhaite que le texte précise lesquelles de ces données peuvent être consultées. KFG redoutant que de plus en plus de tiers non impliqués soient surveillés uniquement parce qu'ils font partie de l'environnement de la personne placée sous surveillance, demande la suppression de cette disposition.

6.1.2 al. 2

Pas de remarques.

6.2. Art. 28 Recherche de personnes condamnées

En dehors d'une procédure pénale, l'autorité compétente peut ordonner une surveillance de la correspondance par poste et télécommunication pour retrouver une personne condamnée à une peine privative de liberté ou qui fait l'objet d'une mesure entraînant une privation de liberté, sur la base d'un jugement définitif et exécutoire, lorsque les autres mesures prises jusqu'alors à cet effet sont restées sans succès ou lorsque les recherches n'auraient aucune chance d'aboutir ou seraient excessivement difficiles en l'absence de surveillance.

---

[122] ZH, LU, SZ, SH, SG, AG, GL, GR, TG, VS, JU, CCDJP, CCPCS, CAPS, SSDP.

[123] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

Différents participants[124] approuvent cette disposition qui vise à étoffer les moyens auxquels l'autorité peut recourir lors de la recherche de personnes condamnées. OW et SO se félicitent en outre de ce que la surveillance prévue ne se limite pas au relevé de données secondaires mais qu'elle permette aussi l'enregistrement de conversations fournissant des indices qui facilitent la localisation de la personne recherchée.

Pour des motifs relevant de la sécurité publique (mise en danger de soi-même et d'autrui), ZG demande que l'on examine s'il ne serait pas judicieux d'étendre cette disposition aux personnes qui font l'objet d'une privation de liberté à des fins d'assistance (art. 397a ss, CC).

Pour privatim, le libellé de cette disposition est trop général au regard du droit régissant la protection des données. Elle ne précise pas qui peut être surveillé ni comment pas plus qu'elle ne stipule où et quand la surveillance peut être exercée. Pourtant elle est susceptible d'induire de graves atteintes aux droits fondamentaux, notamment de personnes gravitant dans l'environnement de la personne condamnée. Aussi, ce participant propose-t-il que les modalités de cette surveillance soient réglées dans le CPP ou l'OSCPT. USS considère que le projet va trop loin lorsqu'il permet de surveiller toutes les personnes qui sont présumées avoir des contacts avec la personne condamnée. Il s'agit là d'une atteinte disproportionnée à la vie privée.

Huit participants[125] souhaitent que le texte précise qu'il doit s'agir d'une personne *en fuite*. Cablecom demande en outre que l'on définisse ce qu'il faut entendre par « n'avoir aucune chance d'aboutir » et « excessivement difficiles ».

FSA relève que celui qui se soustrait à l'exécution d'une peine privative de liberté ou d'une mesure, ne commet pas encore d'infraction. Il est donc capital que l'on respecte le principe de la proportionnalité lorsque l'on est amené à porter des atteintes aussi graves aux droits fondamentaux. A cette fin, on peut se fonder soit sur la gravité de l'acte, soit sur la peine infligée. Si l'on se base sur le premier critère, on peut se référer à la liste des infractions figurant à l'art. 269, al. 2, CPP. Si, en revanche, on considère que la peine infligée est l'élément déterminant, force sera de fixer un seuil à partir duquel une surveillance pourra être ordonnée, par exemple un an de privation de liberté. VD et CP demandent que l'on prenne comme seuil une peine privative de liberté d'au moins six mois.

SIMSA souligne qu'avant que la surveillance soit engagée, personne ne peut savoir quelles conversations livreront des indices et lesquelles n'en livreront pas. Ce constat incite à conclure que soit on s'abstient de toute surveillance, soit on procède à une surveillance générale des conversations. Ce participant relève, en outre, que l'innovation que constitue la possibilité de recourir à la surveillance dans le cadre de la recherche de personnes condamnées engendrera un notable surcroît de travail pour les agents chargés de l'exécution des mesures ad hoc.

AG préconise que l'on remplace « les autres mesures prises » par « les autres recherches entreprises ».

6.3. Art. 29 Procédure

[1] La procédure est régie par analogie par les art. 271 à 279 CPP. La surveillance doit être autorisée par une autorité judiciaire.

[124] ZH, LU, SZ, VD, GE, UR, OW, NW, FR, SO, AR, TI, CCDJP, CCPCS, CAPS, VPSB, SSDP.
[125] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

[2] Les cantons désignent l'autorité qui ordonne la surveillance, l'autorité qui autorise la surveillance et l'autorité de recours.

6.3.1 al. 1

SZ estime qu'il ne se justifie pas de déclarer applicables par analogie les art. 271 à 279 CPP au lieu de 274 à 279 comme c'est le cas actuellement. Il souhaite que l'on précise au niveau de la loi que l'applicabilité par analogie du CPP n'a pas pour effet de conférer à la procédure de recherche dans un cas d'urgence et à la procédure de recherche de personnes condamnées le caractère de procédure pénale, ces deux procédures continuant à relever, l'une du droit administratif et l'autre du droit régissant la police. Le tri d'informations spécifiques sous la direction d'un tribunal dans le but de protéger un secret professionnel n'entre absolument pas en ligne de compte lors de recherches dans des cas d'urgence. Dans le cadre de telles recherches, les informations recueillies à la faveur d'une surveillance limitée à l'identification des participants et aux données du trafic ne peuvent être utilisées que dans le but de sauver les personnes disparues et doivent être détruites dès que le motif de la surveillance a disparu. L'art 29, al. 1, 2ème phrase, statue, en outre, que la surveillance est soumise à autorisation. Il est donc superflu de renvoyer par analogie à l'art. 272 CPP (régime de l'autorisation). Au surplus, un tel renvoi est plutôt de nature à semer la confusion. L'art. 273 CPP traite également de surveillances ordonnées dans le cadre de procédures pénales en cours. De même, le renvoi par analogie à l'art. 279 CPP (obligation de communiquer) en relation avec la clôture d'une recherche dans un cas d'urgence n'a cessé de prêter à discussion. Outre que ce renvoi ne contribue pas à clarifier la norme, l'obligation de communiquer découle des législations cantonales régissant la protection des données et la police et non du CPP. Il n'y pas lieu de réglementer l'ajournement de la communication qui est soumis à l'accord du tribunal des mesures de contrainte. Pire, une telle réglementation entraînerait une confusion de la procédure pénale et de la procédure administrative. Lorsque la police communique à la personne retrouvée ou à ses proches que cette dernière a fait l'objet d'une recherche dans un cas d'urgence, en mettant éventuellement à sa charge les coûts de cette intervention, elle rend une décision qui peut être attaquée devant la juridiction administrative et qui n'est pas sujette à recours au sens des art. 393 à 397 CPP.

UVS estime que le fait de renvoyer globalement au CPP est contraire au système puisque la recherche dans un cas d'urgence est une mesure qui appartient à la politique de sécurité et ne relève pas du droit de la procédure pénale. En outre, poursuit UVS, le fait que la surveillance est soumise à l'autorisation de l'autorité judiciaire est généralement source de problèmes parce qu'il y a souvent « péril en la demeure ». Aussi, la police devrait-elle avoir la compétence d'ordonner les recherches dans un cas d'urgence puisqu'en pareille situation il faut pouvoir agir aussi rapidement que possible. La renonciation à exiger l'autorisation d'une autorité judiciaire peut être compensée par l'octroi à la personne surveillée de la possibilité de former recours a posteriori. En outre, par souci de garantir une répartition aussi claire que possible des attributions, l'autorité compétente pour statuer sur le recours devrait être le juge (de la détention).

6.3.2 al. 2

Pas de remarques.

7. Frais et émoluments

ICT et ePower demandent que les frais occasionnés par les mesures de surveillance soient soumis à une baisse générale et que l'ordonnance sur les émoluments soit adaptée en

conséquence. Cela implique toutefois qu'un processus de bout en bout numérisé soit modélisé dans les directives techniques du service. La sécurité du droit exige que toutes les personnes qui sont parties à un système sachent exactement ce que l'on attend d'elles et à quel moment. Les deux participants proposent que l'on règle ce point avant les débats parlementaires sur le projet.

7.1. Art. 30

[1] Les coûts des équipements nécessaires à la mise en œuvre de la surveillance et les coûts de la surveillance proprement dite sont à la charge des personnes qui exécutent des surveillances en vertu de la présente loi.
[2] L'autorité qui a ordonné la surveillance verse un émolument au service. Le Conseil fédéral fixe les émoluments pour les prestations du service.

7.1.1 al. 1

Plusieurs participants[126] se félicitent de la suppression de l'indemnité à laquelle avaient droit les fournisseurs de service, rappelant notamment que les banques, les fiduciaires, les compagnies d'assurance ne sont pas indemnisées pour la charge qu'implique leur obligation de produire des pièces. Ils estiment qu'une indemnisation est en disharmonie avec le système. ZH fait en outre remarquer que la prévention du blanchiment d'argent occasionne aussi aux banques des frais élevés qu'elles doivent elles-mêmes supporter ou acquitter par prélèvement sur leurs revenus. NW, SO, CAPS et SSDP soulignent, par ailleurs, que par le passé d'importants fournisseurs de services de télécommunication, au demeurant bien organisés, ont gagné des sommes non négligeables grâce aux surveillances de la correspondance par télécommunication.

Inversement, sur le principe, de nombreux participants[127] s'opposent – pour différentes raisons récapitulées ci-après – à la suppression prévue de l'indemnisation pour l'exécution de mesures de surveillance.

La majorité de ces participants[128] relève que la poursuite pénale étant une tâche qui incombe à l'Etat, celle-ci doit être prise en charge par la collectivité. Quelques participants[129] se déclarent non convaincus, en particulier, par l'argument selon lequel une indemnisation serait contraire au système si l'on prend comme point de comparaison les banques, les fiduciaires, les compagnies d'assurance, etc. qui ne sont pas indemnisées pour la charge qu'implique leur obligation de produire des pièces. PS souligne que ce que l'on demande aux fournisseurs de services va nettement plus loin que la production de données et de pièces qui sont, de toute façon, disponibles. JDS et droitsfondamentaux.ch estiment que la comparaison avec l'obligation susmentionnée est erronée car il n'y aurait pas lieu de soumettre les personnes exécutant des surveillances à des obligations spéciales de conservation des données et autres obligations de prêter leur concours, si la production de données pouvait être exigée d'elles sur la base du CPP. Par ailleurs, de l'avis d'ISSS et de MS, cette disposition est contraire aux principes reconnus qui régissent la participation de particuliers à des procès pénaux dirigés contre des tiers, tels que le droit à indemnisation des témoins et des ex-

---

126 ZH, LU, UR, OW, NW, SO, BL, SG, AG, NE, VD, GL, GR, TG, VS, JU, CCDJP, CCPCS, CAPS, SSDP.
127 PS, PDC, PLR, UDC, GPS, PPS, JDS, droitsfondamentaux.ch, RD, ISSS, MS, SIUG, SIMSA, INT, asut, Finecom, Orange, Swisscom, Sunrise, Colt, Verizon, Cablecom, FSA, SKS, Swisscable, CP, CCC, Sitrox, economiesuisse, IT(19), SWICO, hp, COG.
128 PDC, PLR UDC, GPS, asut, Finecom, Orange, Swisscom, Sunrise, Verizon, Cablecom, FSA, SKS Swisscable, SIUG, CP, CCC, Sitrox, PPS.
129 PS, Colt, SiuG, SIMSA, INT, ISSS, PPS, PES.

perts. Pour sa part, MS fait référence à l'art. 434 CPP qui statue expressis verbis que des tiers qui, du fait de l'aide apportée aux autorités pénales, subissent un dommage, ont droit à une juste compensation si ce dommage n'est pas couvert d'une autre manière. En définitive, ces frais font partie intégrante des frais de procédure conformément aux art. 422 ss, CPP, frais qui, à la fin du procès, sont mis à la charge de la personne condamnée.

Un ensemble assez important de participants[130] estime que l'indemnisation des fournisseurs de services de télécommunication contribuera au développement d'une discipline financière qui aura pour effet de freiner les coûts. En effet, l'obligation d'indemniser est de nature à inciter l'autorité compétente à limiter sa propension à ordonner des surveillances.

Un certain nombre de participants[131] soulignent que les entreprises qui fournissent des services de télécommunication doivent mettre en place une infrastructure coûteuse et s'assurer un savoir-faire certain si elles veulent satisfaire aux exigences définies par la loi et prendre en temps utile les mesures techniques nécessaires dans l'hypothèse où elles se verraient confier un mandat par le service. Les investissements auxquels il est indispensable de consentir pour pouvoir exécuter des missions de surveillance posent un problème crucial aux entreprises de moindre envergure voire, comme l'estime PES, représentent pour elles une charge intolérable car il est prévisible qu'ils induisent une augmentation importante des frais de fonctionnement. Pour sa part, Colt est d'avis que l'obligation d'acquérir des équipements qui ne sont utilisés que rarement, voire jamais, constitue une atteinte au principe de la proportionnalité. Dans l'hypothèse où les investissements seraient malgré tout à la charge du fournisseur de services de télécommunication, celui-ci - estime Colt - ne devrait pas être contraint de s'équiper tant qu'il n'a pas reçu de mandat de surveillance. En outre, il y a lieu de laisser au fournisseur de services le soin de déterminer s'il recourra – éventuellement contre rémunération – à des équipements externes même au cas où il serait chargé de missions de surveillance à réitérées reprises. PS fait valoir que les charges liées aux mandats de surveillance se traduisent par une distorsion du marché, qui profite aux grands fournisseurs alors qu'ils occupent déjà une position de quasi-monopole. Aussi exige-t-il que l'indemnisation des fournisseurs de services soit soumise à un régime différencié qui tienne compte de leur capacité de supporter les charges financières découlant des mesures à prendre, cela compte tenu de leur taille.

Cela étant, un nombre non négligeable de participants[132] propose l'adoption d'un libellé aux termes duquel l'autorité qui ordonne les surveillances verse au service un émolument qui comprend les indemnités à verser aux fournisseurs de services.

economiesuisse propose une norme libellée de telle sorte que les fournisseurs de services supportent le coût des équipements dans lesquels ils investissent mais puissent facturer leur utilisation. PDC souhaite que les fournisseurs de services soient indemnisés pour les coûts que leur occasionnent les équipements supplémentaires nécessaires à l'exécution des mandats de surveillance qui leur sont confiés.

Si l'indemnisation des fournisseurs de services est supprimée, la Confédération n'en devra pas moins garantir d'une manière ou d'une autre que ceux-ci continuent de livrer rapidement des données fiables. Telle est la crainte émise par ZG.

---

130 UDC, GPS, asut, Finecom, Orange, Swisscom, Sunrise, Verizon, Cablecom, FSA, SKS, Swisscable, SIUG, CP, CCC, Sitrox, PPS, economiesuisse.

131 PS, Colt, SIUG, SIMSA, INT, ISSS, PPS, GPS.

132 asut, Finecom, Orange, Swisscom, Sunrise, Verizon, Cablecom, Swisscable, IT(19), SWICO, hp, COG.

7.1.2 al. 2

Quand bien même les frais peuvent formellement être mis à la charge des personnes condamnées ou des personnes qui sont tenues de s'en acquitter, ceux-ci, soulignent ZH, LU et ZG, bien souvent, ne peuvent pas être imputés aux parties à la procédure (p. ex. ceux d'une recherche dans un cas d'urgence ou d'une recherche d'une personne condamnée, lorsque le tribunal rend un verdict d'acquittement ou encore dans le cadre d'une procédure d'entraide judiciaire) ou demeurent impayés parce que les personnes concernées sont insolvables. En conséquence, ils sont supportés par les autorités qui ont ordonné la surveillance. Plusieurs participants[133] proposent que l'on fixe de manière adéquate ou que l'on abaisse notablement les tarifs prévus par l'ordonnance du 7 avril 2004 sur les émoluments et les indemnités en matière de surveillance de la correspondance par poste et télécommunication[134]. SZ fait valoir que, dans ce contexte, le service ne devrait pas assumer d'inutiles fonctions d'interface, telles que le contrôle du respect du délai de conservation des données et la transmission d'informations relatives à des raccordements de télécommunication. LU et ZG demandent qu'on leur donne, le moment venu, la possibilité de s'exprimer sur l'ordonnance concernant les émoluments. FR entend que la question des émoluments que les cantons doivent verser au service soit soumise à un examen à la lumière d'une évaluation qui doit encore être réalisée. VD part de l'idée que le fait que le bénéficiaire des émoluments reste le service, devrait induire un excédent des coûts. NE demande que l'on examine la possibilité d'abolir l'obligation de payer des émoluments à laquelle sont soumises les autorités qui ordonnent la surveillance. Enfin, pour PS, il y a lieu de veiller à ce que le montant des émoluments ne soit pas prohibitif pour les autorités de poursuite pénale, de manière à ce que les forfaits prévus par cas ne les dissuadent pas d'ordonner des enquêtes pourtant essentielles.

8. Dispositions pénales

8.1. Art. 31 Contraventions

[1] Est puni d'une amende de 100 000 francs au plus quiconque, intentionnellement:

a. ne donne pas suite aux injonctions du service;

b. ne respecte pas l'obligation de conserver des données mentionnée aux art. 19, al. 2 et 23.

[2] La tentative et la complicité sont punissables.

[3] Si l'auteur agit par négligence, il est puni d'une amende de 40 000 francs au plus.

[4] Les art. 102 al. 1, 3 et 4 CP et 112 CPP sont applicables par analogie. L'amende est de un million de francs au plus.

Sur le principe, SO et CP souscrivent aux dispositions proposées. Aux yeux de CP, elles présupposent, toutefois, que la loi prévoie une indemnité et une certification gratuite pour les personnes chargées de l'exécution de surveillances.

PES et SKS estiment que les dispositions pénales sont nettement trop strictes, notamment parce que les personnes qui sont chargées d'exécuter des surveillances n'ont guère de moyens de s'opposer aux injonctions du service. Pour cette raison et compte tenu de la tendance à l'exécution de surveillances de plus en plus nombreuses, la norme pénale préconisée aboutirait à ce que les fournisseurs de services de télécommunication soient arbitrairement soumis aux ordres de l'autorité. En outre, la quotité des peines prévues pourrait mettre en péril l'existence des fournisseurs de moindre envergure. Ils demandent donc que la sévérité de la disposition pénale proposée soit nettement atténuée.

---

133 ZH, LU, ZG, BL, AG, TI, GL, GR, TG, VS, JU, SZ, OW, CCDJP, CCPCS.
134 RS 780.115.1

Dans ce contexte, plusieurs participants[135] soulignent que les obligations incombant aux personnes qui exécutent des surveillances ne sont pas réglées de manière précise. Dans ces conditions, il est délicat d'adopter la disposition pénale proposée, estime PLR. SIMSA est de l'avis qu'il manque à celle-ci des éléments constitutifs univoques permettant de justifier une sanction pénale. Aux yeux de quelques participants[136], la norme non seulement viole le principe de précision, mais encore elle présume qu'en vertu de l'art. 15, let. a, AP le service doit donner lui-même des injonctions (directives et décisions) supplémentaires même s'il ne peut être lui-même à l'origine de l'ordre de surveillance.

Enfin, Orange et Colt estiment qu'il n'est pas approprié que les personnes physiques soient aussi soumises à cette disposition. Ces deux participants proposent donc de restreindre le champ d'application personnel de la LSCPT et, partant, de ses dispositions pénales, aux personnes morales.

8.1.1 al. 1

Plusieurs participants[137] plaident en faveur d'une norme plus sévère. OW émet des doutes quant à savoir si la norme proposée aura l'efficacité visée. NW et CAPS estiment que le fait que l'avant-projet érige les infractions en contraventions est inadapté et n'a pas d'effet dissuasif si l'on prend en compte le rapport existant entre les bénéfices réalisés dans le domaine des télécommunications et les coûts occasionnés par les surveillances. En effet, dans certains cas, l'amende maximale prévue (100'000 francs) pour réprimer la violation d'obligations est plus que contrebalancée par les économies réalisées grâce à cette infraction. Ce constat incite quelques participants[138] à demander que l'on augmente le montant maximum de l'amende, une majorité d'entre eux[139] proposant même de le porter à 1 million de francs.

let. a

Huit participants[140] estiment que, sous l'angle du principe de précision statué à l'art. 1 CP, la formulation «(…) quiconque, intentionnellement, ne donne pas suite aux injonctions du service » appelle des réserves du point de vue des valeurs qui fondent l'Etat de droit.

let. b

VD, BL et AG souhaitent que l'applicabilité de la disposition soit étendue aux infractions à l'art. 20 AP; AG plaide pour qu'elle le soit en outre aux infractions à l'art. 22 AP.

8.1.2 al. 2

UNIZH estime que la punissabilité de la tentative et de la complicité n'est pas conforme à notre système pénal puisqu'en l'occurrence il s'agit de contraventions et non de délits ou de crimes.

---

135 PLR, SIMSA, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
136 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
137 ZH, LU, AG, GL, GR, TG, VS, JU, NW, CCDJP, CAPS.
138 ZH, AG, LU, GL, GR, TG, VS, JU, CCDJP.
139 AG, LU, GL, GR, TG, VS, JU, CCDJP.
140 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

8.1.3 al. 3 et 4

Pas de remarques.

8.2. Art. 32 Juridiction

La poursuite et le jugement des infractions au sens de l'art. 31 incombent aux cantons.

CCPCS se félicite expressément de ce que la compétence juridictionnelle soit attribuée aux cantons, ce qui est conforme au principe selon lequel la poursuite et le jugement des infractions pénales ressortissent à ces derniers.

S'agissant de la compétence rationae loci, quelques participants[141] souhaitent que celle-ci soit établie au lieu où le fournisseur de services défaillant offre sa prestation. S'il le fait dans plusieurs cantons, il y a lieu de désigner une juridiction fédérale.

BL et CAPS ne voient pas pourquoi la juridiction serait cantonale. Ils proposent que la poursuite et le jugement des infractions en cause ressortissent de manière générale à une juridiction fédérale. BL fait remarquer que l'art. 31 AP vise à réprimer des contraventions dans des domaines relevant de la compétence du service et donc, par principe, de la Confédération. A cela s'ajoute qu'en règle générale les manquements des fournisseurs de services, qui sont visés par cette disposition, touchent plusieurs cantons. Selon CAPS, le recours contre les décisions du service est recevable selon les règles de la procédure fédérale, de sorte que les dispositions du droit pénal administratif devraient être applicables également aux procédures pénales.

9. Surveillance et voies de droit

9.1. Art. 33 Surveillance

[1] Le service veille à ce que la législation relative à la surveillance de la correspondance par poste et télécommunication soit respectée.

[2] S'il constate une violation du droit, il peut, par analogie, prendre les mesures prévues à l'art. 58, al. 2, let. a de la loi du 30 avril 1997 sur les télécommunications. Il peut ordonner des mesures provisionnelles.

De l'avis de plusieurs participants[142], la formule « Le service veille à ce que la législation (…) soit respectée », utilisée à l'al. 1, est en contradiction avec l'art. 15, let. a, AP selon lequel le service n'a précisément pas la compétence de vérifier si un ordre de surveillance est conforme au droit. Aussi, l'art. 33 AP doit-il être interprété en ce sens que le service n'a pas à assurer, de manière générale, le respect du droit en cause et qu'il lui incombe seulement de garantir que les fournisseurs de services de télécommunication se conforment à la loi. Le libellé de l'al. 2 incite d'ailleurs à cette interprétation. En d'autres termes, le service devrait assumer le rôle qui incombe à l'administration interposée entre l'autorité qui ordonne la surveillance et le fournisseur de services, et appliquer la loi. En outre, il doit pouvoir trancher dans les cas litigieux, ce qu'il n'a pas la compétence de faire aujourd'hui. Toutefois, il ne se reconnaît pas dans ce rôle. En effet, plus le temps passe et plus il agit comme s'il était une autorité de surveillance. Il se borne à émettre des directives techniques et à édicter les prescriptions d'ordre organisationnel et administratif qu'il lui incombe d'établir à titre de pures dispositions d'exécution. Il ne règlerait donc pas la forme sous laquelle les fournisseurs de services doivent présenter certaines données mais édicterait de plus en plus de prescriptions

[141] ZH, LU, SG, GL, GR, TG, VS, JU, CCDJP.
[142] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, SWICO, hp, COG.

qui définissent ce que l'on attend d'eux en général. Les participants en question déplorent, en outre, que le service fasse parfois preuve d'un zèle excessif en allant jusqu'à exiger, par mesure de précaution, la fourniture de prestations qui vont au-delà de ce que demandent les autorités chargées des enquêtes. La tendance prise par le service à devenir de plus en plus autonome sans qu'aucun moyen de droit ni aucune autorité de surveillance permette de contrôler son activité, ne laisse pas d'inquiéter certains participants. Ceux qui s'expriment à propos de l'art. 33 AP, relevant que, dans l'ensemble, l'avant-projet est abstrus, donc pas satisfaisant, arrivent à la conclusion qu'il faut revoir complètement l'art. 33 puisque le service lui-même ne se considère pas comme un gardien du droit mais plutôt comme un organe qui s'efforce d'assurer autant de surveillances que possible. Or ce rôle n'est pas compatible avec la fonction d'autorité de surveillance.

Cablecom critique le libellé choisi qui soumettrait l'activité du service à la propre surveillance de celui-ci. Elle propose de désigner l'Office fédéral de la communication (OFCOM) en qualité d'autorité de surveillance.

Rappelant l'affaire des fiches, KFG veux avoir la certitude que l'activité du service soit soumise à un contrôle. Dans cet esprit, il propose l'instauration d'un organe de contrôle qui vérifie à intervalles réguliers les dépenses du service de même que la proportionnalité et la légalité des mesures ordonnées.

9.2. Art. 34 Voies de droit

[1] Les décisions du service sont sujettes à recours conformément aux dispositions générales de la procédure fédérale.

[2] Le recourant n'est pas habilité à recourir contre une décision du service lui enjoignant d'exécuter une surveillance en invoquant l'illégalité de l'ordre de surveillance sur lequel cette décision se fonde. Il peut en revanche faire valoir contre les décisions du service des questions d'ordre technique ou organisationnel liées à l'exécution de la mesure de surveillance ordonnée.

9.2.1 al. 1

Pas de remarques.

9.2.2 al. 2

Neuf participants[143] soulignent que la disposition proposée répond à un besoin d'ordre pratique. Pour CAPS, le fait d'exclure de manière générale le contrôle de légalité va, cependant, trop loin. Les fournisseurs de services de télécommunication devraient avoir la possibilité d'invoquer que les mesures ordonnées sont illégales puisque l'autorité qui autorise la surveillance ne dispose pas des connaissances techniques nécessaires.

Un grand nombre de participants[144] exige que, contrairement au libellé de l'al. 2, le recourant puisse, de manière générale, faire contrôler la légalité d'un ordre de surveillance.

Quelques participants[145] relèvent qu'une surveillance ordonnée illégalement - par exemple, dans le but de poursuivre une infraction qui n'est pas énumérée dans la liste figurant à l'art.

---

143 LU, NW, GL, GR, TG, VS, JU, CCDJP, CAPS.

144 ZG, BE, BL, AR, PLR, PS, economiesuisse, UVS, privatim, UVS, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom, Swisscable, SKS, SIUG, VPSF, SWICO, hp, COG, IT(19), ISSS.

145 ZG, privatim, PS, PLR, economiesuisse, UVS.

269, al. 2, let. a, CPP ou parce que la mesure qu'elle implique n'est pas prévue dans la loi - porte atteinte aux droits de la personne concernée. En outre, l'intérêt public commande qu'elle puisse être dénoncée devant le juge étant donné la gravité de l'atteinte aux droits fondamentaux dont elle est la cause. Enfin, ces participants rappellent que lorsqu'il y a péril en la demeure, les autorités de poursuite pénale peuvent requérir une surveillance durant la procédure de recours, cela à titre de mesure provisionnelle. Ils ajoutent que le juge peut lever l'effet suspensif d'un éventuel recours.

BE estime choquant que les personnes auxquelles le service a, par erreur, enjoint d'exécuter une surveillance, ne puissent recourir contre une telle décision.

Huit participants[146] font observer que, selon les règles générales de la procédure fédérale, l'autorité de recours ne saurait avoir un pouvoir d'examen plus large que celui de l'autorité de première instance. Comme le service ne jouit d'aucun pouvoir d'examen sur le fond, ce qui signifie qu'il se borne à reprendre à son compte les ordres de surveillance, les autorités de recours n'examineront pas les points laissés de côté par l'instance précédente. Il résulte de ce qui précède que les décisions du service ne sont pas sujettes à recours. Aussi, les participants en cause exigent-ils que l'on aménage des compétences ad hoc permettant d'examiner l'activité du service (v. également supra, partie III, ch. 3.2.1, remarques concernant l'art. 15, let. a, AP).

Cablecom est de l'avis qu'il y a lieu de biffer purement et simplement l'al. 2 parce qu'il est contraire aux dispositions de la procédure fédérale. Swisscable fait observer qu'un cahier des charges ne sert à rien s'il n'existe pas de base légale permettant, au besoin, de réclamer en justice le respect des droits et des obligations qui y sont consignés. Aussi, par souci de garantir la sécurité du droit, importe-t-il d'ouvrir la voie du recours contre les ordres de surveillance excessifs émanant de l'autorité. Ni la loi en vigueur ni l'avant-projet n'offrent cette possibilité, d'où un manque de sécurité du droit.

Un nombre relativement important de participants[147] préconisent le nouveau libellé suivant: « Le recourant n'est pas habilité à recourir contre une décision du service lui enjoignant d'exécuter une surveillance en invoquant que l'ordre de surveillance est, en l'espèce, contraire au principe de la proportionnalité ou que l'autorité qui a ordonné la surveillance a outrepassé son pouvoir d'appréciation ».

BL relève en outre que si la faisabilité d'une mesure sous les angles technique et organisationnel au sens de l'al. 2, constitue un motif de recours, il y a logiquement lieu d'examiner celle-ci avant d'ordonner cette mesure. Il y a lieu de compléter en conséquence l'art. 15, let a, AP (v. supra, partie III, ch. 3.2.1, remarques concernant l'art. 15, let. a, AP).

AG demande l'instauration d'un autre moyen de contrôle pour le cas où les fournisseurs de service ne seraient pas habilités à invoquer l'illégalité de l'ordre de surveillance. De l'avis d'OW, il importe que ceux-ci puissent faire contrôler si le service s'est acquitté de ses tâches conformément à l'art. 15 AP. Or cette possibilité ne ressort pas clairement de l'avant-projet.

---

146 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SKS.

147 economiesuisse, SWICO, hp, COG, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, IT(19).

10. Dispositions finales

10.1. Art. 35 Exécution

Le Conseil fédéral et, dans la mesure où ils sont compétents, les cantons édictent les dispositions nécessaires à l'exécution de la présente loi.

Pas de remarques.

10.2. Art. 36 Abrogation et modification du droit en vigueur

L'abrogation et la modification du droit en vigueur sont réglées à l'annexe.

Les remarques concernant les modifications du droit en vigueur sont récapitulées au ch. 11, infra.

10.3. Art. 37 Disposition transitoire

Les surveillances ordonnées avant l'entrée en vigueur de la présente loi sont régies selon le nouveau droit.

Plusieurs participants[148] de la branche des services de télécommunication exigent que l'on fixe des délais transitoires convenables pour la mise en œuvre des nouvelles dispositions sur le plan technique. Ils proposent la nouvelle formulation suivante: « Les surveillances ordonnées avant l'entrée en vigueur de la présente loi sont régies selon *l'ancien* droit. *A la date de l'entrée en vigueur du nouveau droit, les surveillances ordonnées selon l'ancien droit ne peuvent être poursuivies qu'à condition qu'elles soient également licites selon le nouveau droit ».* Eu égard au fait que le champ d'application tant matériel que personnel sera élargi, switch et switchplus préconisent l'instauration d'un délai transitoire approprié pour les personnes qui seront, pour la première fois, chargées d'exécuter des mesures de surveillance. Ils proposent donc l'adjonction d'un al. 2 libellé comme suit: *« Les personnes, qui par suite de l'élargissement du champ d'application matériel ou personnel, sont tenues pour la première fois de mettre en œuvre des mesures de surveillance disposent d'un délai d'une année à compter de l'entrée en vigueur de la présente loi pour s'exécuter ».*

Selon BL, la formulation de la disposition prête à malentendu. Il part de l'idée qu'à la date de l'entrée en vigueur de la loi, le nouveau droit s'appliquera à toutes les surveillances *en cours* qui auront été ordonnées avant cette entrée en vigueur et non, rétroactivement, à toutes les surveillances qui l'auront été avant cette date.

Dans le même ordre d'idées, SZ demande si la communication prévue à l'art. 11 AP devra être rattrapée dans l'hypothèse où le nouveau droit serait également applicable aux surveillances qui ont été closes.

Aux yeux de Cablecom, l'application rétroactive du nouveau droit aux surveillances en cours, telle qu'elle est prévue à l'art. 37 AP, est problématique puisque, par exemple, il n'est pas impossible que les données rétroactives obtenues lors de ces surveillances ne remontent pas encore à douze mois. Aussi, ce participant propose-t-il le nouveau libellé suivant: « Les surveillances ordonnées avant l'entrée en vigueur de la présente loi sont régies selon *l'ancien* droit. *Les surveillances ordonnées après l'entrée en vigueur de la présente loi sont*

[148] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

régies selon l'ancien droit durant une période transitoire de six mois »

Selon MS, la disposition va à l'encontre du principe de précision voulant que le citoyen soit informé des conséquences qu'aura pour lui tel ou tel comportement. Aussi, estime ce participant, la nouvelle LSCPT ne doit-elle valoir que pour les surveillances ordonnées à compter de son entrée en vigueur.
D'autres participants[149] soupçonnent une inadvertance. A leurs yeux, telle qu'elle est formulée, cette disposition signifie indubitablement que les surveillances en cours qui ont été *ordonnées* avant l'entrée en vigueur de la nouvelle loi sont régies par les dispositions de celle-ci, à compter de son entrée en vigueur. Se référant au rapport explicatif, ils estiment cependant que cette disposition est superflue.

10.4. Art. 38 Référendum et entrée en vigueur

[1] *La présente loi est sujette au référendum*.
[2] *Le Conseil fédéral fixe la date de l'entrée en vigueur*.

Pas de remarques.

11. Abrogation et modification du droit en vigueur (annexe ; art. 36 AP)

11.1. Code de procédure pénale suisse du 5 octobre 2007 (CPP)[150]

11.1.1 Art. 269, al. 2, let. a Conditions

[2] *Une surveillance peut être ordonnée aux fins de poursuivre les infractions visées par les dispositions suivantes:*
a. *CP19: art. 111 à 113; 115; 118, ch. 2, 122; 127, 129; 135; 138 à 140; 143; 144, al. 3; 144bis, ch. 1, al. 2, et ch. 2, al. 2; 146 à 148; 156; 157, ch. 2; 158, ch. 1, al. 2, et ch. 3; 160; 161; 163, ch. 1; 180; 181 à 185; 187; 188, ch. 1; 189 à 191; 192, al. 1; 195; 197; 220; 221, al. 1 et 2; 223, ch. 1; 224, al. 1; 226; 227, ch. 1, al. 1; 228, ch. 1, al. 1 à 4; 230bis; 231, ch. 1; 232, ch. 1; 233, ch. 1; 234, al. 1; 237, ch. 1; 238, al. 1; 240, al. 1; 242; 244; 251, ch. 1; 258; 259, al. 1; 260bis à 260^{quinquies}; 261bis; 264 à 267; 271; 272, ch. 2; 273; 274, ch. 1, al. 2; 285; 301; 303, ch. 1; 305; 305ter, ch. 2; 310; 312; 314; 317, ch.1; 319; 322^{quater}; 322^{septies}; 322$^{...}$;*

Douze participants[151] se félicitent expressément de l'adjonction de l'art. 220 CP (enlèvement de mineur) à la liste des infractions.

Pour l'USS, l'AP va au-delà de l'objectif fixé. Ainsi, la liste des infractions est pléthorique. A l'évidence, il ne se justifie pas que la Confédération puisse mettre en place des « Government Software » (souvent aussi appelés « chevaux de Troie ») lors d'infractions telles qu'un dommage à la propriété lorsqu'il est de grande ampleur ou encore une entrave au service des chemins de fer.

SIUG et Swiss Privacy Foundation relèvent qu'à l'heure actuelle déjà la liste exhaustive des infractions n'est pas applicable lorsque l'une des infractions visées a été commise via Internet. En pareil cas, les personnes qui exécutent des surveillances de la correspondance par télécommunication doivent, en vertu de l'art. 20, al. 3, AP, fournir au service toute indication permettant d'identifier l'auteur. Ces deux participants demandent que l'on s'interroge de manière critique sur l'opportunité d'étendre cette disposition à des infractions susceptibles de

149 GL, GR, TG, VS, JU, CCDJP, CAPS.
150 RO 2010 1881; en vigueur depuis le 1.1.2011.
151 LU, ZH, OW, NW, GL, GR, TG, VS, JU, CCPCS, CCDJP, CAPS.

donner lieu à une surveillance. Il importe, en outre, que la liste des infractions valle également pour l'accès aux données conservées.
KFG ne voit aucune raison justifiant l'adjonction de l'enlèvement de mineur (art. 220 CP), à la liste des infractions. Les éléments constitutifs ne correspondent pas à ceux d'une infraction grave. Aussi convient-il de radier l'art. 220 CP de la liste.

CFMJ souhaite que la liste des infractions soit complétée par l'art. 55, al. 1, let a de la loi fédérale du 18 décembre 1998 sur les jeux de hasard et les maisons de jeu (loi sur les maisons de jeu, LMJ)[152] au motif qu'il est de plus en plus fréquent que des maisons de jeux soient exploitées illégalement sur Internet. Pour pouvoir assurer une poursuite pénale efficace de ces maisons de jeux, il est nécessaire de disposer de nouveaux moyens d'enquête. Afin de collecter les moyens de preuve, il est indispensable de pouvoir s'infiltrer dans le réseau de ces maisons de jeu illégales et ce d'une manière analogue à celle qui est employée lors d'une perquisition. Si, dans la réalité, il est possible de procéder à une perquisition sur la base de l'art. 56 LMJ, dans le monde virtuel, en revanche, cela est impossible faute de mesures de surveillance au sens de la LSCPT. Pourtant de telles mesures sont indispensables dans le cadre de poursuites pénales à l'encontre de maisons de jeu exploitées illégalement sur Internet. CFMJ estime que l'art. 55, al. 1, LMJ répond aux critères justifiant son adjonction à l'art. 269, al. 2, CPP car il vise un délit d'une gravité particulière qui est de plus en plus souvent commis via Internet.

11.1.2 Art. 270bis CPP Interception et décryptage de données *(nouveau)*

[1] Lorsque, dans le cadre d'une surveillance de la correspondance par télécommunication, les mesures de surveillance prises jusqu'alors sont restées sans succès ou lorsque les autres mesures de surveillance n'auraient aucune chance d'aboutir ou rendraient la surveillance excessivement difficile, le ministère public peut ordonner, même à l'insu de la personne surveillée, l'introduction dans un système informatique de programmes informatiques permettant d'intercepter et de lire des données. Dans son ordre de surveillance, le ministère public indique le type de données qu'il souhaite obtenir.

[2] L'ordre de surveillance est soumis à l'autorisation du tribunal des mesures de contrainte.

Quatorze participants[153] se félicitent de la nouvelle disposition. Quelques-uns d'entre eux[154] soulignent que la problématique du cryptage a tendance à se répandre fortement. UVS se déclare opposé à l'instauration de la condition supplémentaire que constitue ce qu'il est convenu d'appeler la « double subsidiarité », condition trop ambitieuse et, partant, peu viable. Le recours à des « Government Software » (souvent aussi appelés « chevaux de Troie ») n'est pas plus incisif que d'autres mesures de surveillance, notamment celles qui sont visées à l'art. 280 CPP. Ce participant ne voit pas pourquoi sous le prétexte de « subsidiarité », on devrait procéder à l'écoute des raccordements de téléphonie fixe et des communications par téléphone mobile d'un prévenu avant de surveiller les appels passés au moyen de la téléphonie sur Internet. Le contrôle de la proportionnalité qu'implique l'art. 269 CPP apparaît suffisant.

Dix participants[155] s'opposent catégoriquement à l'introduction de programmes informatiques dans un système informatique appartenant à des tiers; d'autres[156] émettent des réserves à ce sujet.

---

[152] RS 935.52
[153] ZH SZ, NW, OW, GL, GR, TG, VS, JU, CCDJP, CCPCS, CAPS, SPICT, UVS.
[154] ZH, GL, GR, TG, VS, JU, CCDJP, CCPCS.
[155] GPS, JDS, droitsfondamentaux.ch, Cablecom, CCC, SKS, SIUG, KFG, PPS, ISSS.
[156] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, ZH, BL, AR, LU, PS, SIUG, privatim, economiesuisse, Swisscable.

PES, JDS, droitsfondamentaux.ch, SKS et SIUG font d'emblée observer que l'introduction de programmes informatiques n'est pas autre chose que l'implantation dans l'ordinateur de particuliers de logiciels destinés à le détériorer. C'est dire qu'un tel agissement constitue une grave atteinte à la vie privée des victimes. En effet, ce moyen de surveillance permet d'accéder à l'ensemble des fichiers d'un système informatique (photos, correspondance, mots de passe, microphone, etc.). Ces participants jugent incompréhensible ou, plus exactement, révélateur le fait que, nulle part, il n'est fait référence à l'arrêt de principe rendu en février 2008 par la Cour constitutionnelle allemande[157], selon lequel le recours à ce moyen porte atteinte au droit fondamental à la confidentialité et à l'intégrité des données traitées dans un système informatique, droit qui découle du droit général à la protection de la personnalité. La Cour constitutionnelle n'entend autoriser la « perquisition en ligne » que s'il y va de la protection de biens juridiques primordiaux tels que l'intégrité corporelle, la vie et la liberté des personnes concernées ou encore des biens collectifs dont la mise en péril est de nature à saper les fondements de l'Etat voire à peser sur son existence-même ou encore à porter atteinte aux garanties fondamentales qui entourent l'existence des individus. De l'avis des participants susmentionnés, ce droit fondamental découlerait de l'art. 10 Cst.

SIUG fait en outre référence à la Cour fédérale de justice allemande qui, à la lumière du droit fédéral en vigueur, considère que l'application d'une telle mesure de surveillance à des fins de poursuite pénale, est illicite. A l'appui de son prononcé[158], elle fait valoir que cette surveillance est exécutée à l'insu de la personne concernée alors que pour une perquisition classique la loi exige la présence de témoins et des détenteurs des locaux. C'est d'ailleurs ce que prévoit l'art. 245 CPP (Exécution de la perquisition).

Par ailleurs, PES, JDS, droitsfondamentaux.ch et SKS critiquent le fait que la perquisition d'ordinateurs n'est pas censée être limitée à des programmes déterminés tels que la messagerie. Une limitation à des fonctions précises exige toutefois une perquisition de la totalité du disque dur afin d'identifier les données apparemment intéressantes. Par ailleurs, l'argument de la « double subsidiarité » n'est pas convaincant. En effet, la surveillance usuelle de la correspondance par télécommunication est, elle aussi, liée à la condition que les autres mesures prises jusqu'alors soient restées sans succès ou n'aient aucune chance d'aboutir. En d'autres termes, cela revient à dire qu'en cas d'échec des mesures de surveillance usuelles, les autorités chargées de l'enquête et le tribunal compétent pour autoriser la surveillance sont presque automatiquement fondés à autoriser une exploration plus poussée de l'ordinateur concerné. Par ailleurs, il n'est pas prévu non plus d'établir une liste particulière d'infractions puisque, comme le précise le rapport explicatif, toutes les infractions qui pourraient autoriser une surveillance normale de la correspondance téléphonique sont « susceptibles, dans un cas particulier, de présenter une gravité justifiant d'avoir recours au procédé de surveillance » visé à l'article 270bis CPP. Le rapport ne précise toutefois pas en quoi doit consister la gravité particulière en question. Les participants susmentionnés en tirent sans hésiter la conclusion que les auteurs de l'avant-projet ont voulu créer ainsi une base légale permettant de mettre aisément en œuvre un procédé viable sur le plan technique. Le recours à ce procédé soulève la question de la protection juridique des personnes concernées. Il amène aussi à s'interroger sur l'efficacité que l'on peut en attendre. Il est prévisible que les personnes qui sont censées faire l'objet de telles mesures de surveillance cherchent à y échapper. Elles peuvent prendre des mesures de précaution ou utiliser des canaux de communication autres que leur propre ordinateur.

PES, SKS, KFG et PPS redoutent que le procédé qui consiste à introduire des programmes

---

157 BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333).
158 BGH, arrêt du 31.1.2007 – StB 18/06.

informatiques dans l'ordinateur d'un tiers ne crée dans le système de sécurité une brèche par laquelle, tôt ou tard, des criminels pourront aussi s'infiltrer. Ainsi, il n'est pas exclu que le logiciel-source du « cheval de Troie » installé par les autorités fasse son apparition sur la toile pour être ensuite utilisé abusivement par des criminels.

KFG relève que tout logiciel qui est implanté sur un système met en péril celui-ci. En outre, il peut nuire à la sécurité de l'ordinateur, voire de l'ensemble du réseau. Dans ce contexte, une question se pose : comment une autorité entend-elle prouver que la pièce à conviction qui a été découverte n'a pas été téléchargée ni envoyée par le « cheval de Troie » lui-même. S'il est vrai, en effet, que des données peuvent être lues, il est aussi exact qu'elles peuvent également être interceptées, écrites ou modifiées, ce qui fait obstacle à une administration des preuves.

PPS souligne qu'il est impossible de déterminer précisément à l'avance comment le « cheval de Troie » et d'autres éléments du système informatique interagiront, ce qui débouche sur la question suivante : qui doit répondre du dommage causé par « un cheval de Troie » mis en place par la Confédération?

CCC estime qu'en voulant recourir lui-même à des logiciels du type « cheval de Troie » qu'il est interdit de commercialiser en Suisse, l'Etat « dépasse les bornes ». En outre, des tiers intègres doivent s'attendre à ce que leur ordinateur soit atteint car, selon le réseau de communication utilisé, des tiers sont impliqués. L'utilisation de « chevaux de Troie » par l'Etat a quelque chose d'outrecuidant et la probabilité que des tiers (innocents) soient aussi surveillés est par trop grande.

SIUG, lui aussi, énumère en détail les difficultés techniques et les risques liés à l'installation de tels logiciels dans les ordinateurs des personnes sous surveillance. Ce participant estime, en outre, que les autorités suisses ne sauraient s'accommoder du risque qu'elles déclenchent une contamination par des logiciels nuisibles des systèmes informatiques d'un nombre relativement important de personnes, également à l'étranger.

Sept participants[159] déplorent l'absence de normes réglant les modalités d'effacement des programmes en cause des ordinateurs dans lesquels ils ont été introduits. Pour ZH, BL, ZG et PS, une autre question n'est pas réglée: celle des exigences auxquelles doit satisfaire la sécurité des programmes d'interception et de décryptage des données et celle de leurs fournisseurs.

Pour PLR, economiesuisse et Swisscable, les incidences qu'auront les « chevaux de Troie » sont difficilement prévisibles. Les deux derniers exigent que seule soit autorisée l'introduction de programmes dont la fonction se limite à la surveillance des secteurs agréés par l'autorité et qui ne perturbent pas le fonctionnement d'autres logiciels. Ils estiment que la Confédération doit répondre d'éventuels dommages. Ils proposent tous les deux des dispositions rédigées.

Aux yeux de l'UDC, les atteintes à la sphère privée de personnes et d'entreprises, qui découlent de l'utilisation de tels programmes, constituent une ultima ratio. Aussi, les exigences et les critères auxquels doit obéir le recours à de tels procédés doivent-ils être élevés. Or la disposition proposée ne remplit pas ces exigences. Ce parti propose de définir explicitement dans la loi les infractions qui autorisent l'utilisation de ces procédés. Quant au PDC, il émet certaines réserves quant à l'emploi de méthodes qui permettent de « ratisser large » ou qui représentent un risque non négligeable pour les tiers non concernés par l'enquête.

---

[159] ZH, BL, AR, ZG, PS, SIUG, privatim.

privatim, également, souligne la gravité de l'atteinte à la sphère privée. Sous l'angle constitutionnel, l'Etat n'a, par principe, pas à fouiller dans les systèmes informatiques des justiciables. Aussi, une base légale qui autorise l'introduction d'un programme informatique dans un système informatique, à l'insu de la personne surveillée, doit-elle répondre aux exigences les plus rigoureuses au regard du principe de précision. Or la disposition proposée ne remplit pas ces exigences à tous les égards. privatim et le PS, se référant à l'arrêt de la Cour constitutionnelle allemande[160], demandent que la liste des infractions figurant à l'art. 269, al. 2, let. a, CPP, soit limitée à quelques infractions très graves contre la vie et l'intégrité corporelle ou contre l'intégrité de l'Etat. Pour leur part, BS et FR demandent que, d'une manière générale, la liste des infractions soit raccourcie pour ce qui est de la possibilité de recourir à des « chevaux de Troie » ; FR, de surcroît, entend que de telles atteintes à la sphère privée ne soient autorisées qu'à des conditions très strictes, c'est-à-dire uniquement en présence d'indices concrets qu'un bien juridique essentiel sera mis en péril de manière imminente et pas seulement, comme le prévoit l'art. 269, al. 1, let. a, CPP, lorsque de graves soupçons laissent présumer que l'une des infractions figurant dans la liste a été commise. En outre, toujours selon FR, les autorités de la Confédération doivent évaluer l'ampleur que prendront ces mesures par rapport à l'ensemble des mesures de surveillance qu'elles peuvent ordonner.

BE demande que la loi précise si le recours à des « chevaux de Troie » autorise à procéder à une « perquisition électronique » ou si seules les données relatives au trafic peuvent être relevées.

MS fait observer que le libellé de la disposition proposée permet de relever tous les types de données, d'où la proposition d'intégrer cette disposition à l'art. 280 CPP. En outre, ce libellé ne précise pas si l'applicabilité de la disposition est limitée aux infractions énumérées dans la liste figurant à l'art. 269, al. 2, let. a, CPP.

UNISG et UNIZH émettent des réserves de principe quant à l'utilisation de ce procédé de surveillance. Ils soulignent, en outre, le défi particulier que représente une telle surveillance tant sur le plan organisationnel que pour les personnes qui y participent.

ISSS met l'accent sur le fait qu'à son sens le recours aux programmes informatiques de surveillance est propre à faire baisser notablement le niveau de protection des données et de sécurité informatique atteint en Suisse.

11.1.3 Art. 270ter CPP Utilisation de systèmes de localisation *(nouveau)*

[1] Le ministère public peut ordonner l'utilisation par la police d'appareils permettant de déterminer les données d'identification spécifiques des appareils de téléphonie mobile et de les localiser. Les appareils utilisés doivent au préalable avoir fait l'objet des autorisations nécessaires.

[2] L'ordre de surveillance est soumis à l'autorisation du tribunal des mesures de contrainte.

Sur le principe, un nombre relativement important de participants[161] se félicite de cette nouvelle disposition.

Quelques-uns[162] proposent de remplacer les termes « appareils de téléphonie mobile » par l'expression « moyens de communication mobiles », de manière à couvrir également les instruments issus des nouvelles technologies, tels que les notebooks équipés de cartes SIM. CCPCS propose l'adjonction d'un al. 3 qui permette l'utilisation d'appareils de localisation

160 BVerfG, 1 BvR 370/07 du 27.2.2008, Absatz-Nr. (1 - 333).
161 ZH, LU, SZ, OW, NW, SG, BL, GL, GR, TG, VS, JU, CCDJP, CCPCS, CAPS.
162 ZH, LU, CCDJP, GL, GR, TG, VS, JU, CCPCS.

lors de recherches dans un cas d'urgence. D'autres participants [163] soulignent que les appareils de localisation visés sont des dispositifs techniques de surveillance qui sont utilisés par la police et non par le service. Cela étant, ils proposent d'intégrer la disposition à l'art. 280 CPP et de prévoir une procédure d'autorisation ad hoc.

PES, JDS, droitsfondamentaux.ch, SKS et SIUG rejettent la disposition en faisant observer que l'IMSI-catcher[164], lorsqu'il est utilisé, non seulement permet l'identification du téléphone mobile d'un usager déterminé mais encore détourne (et perturbe) les communications sur un réseau de téléphonie mobile de l'ensemble des personnes – suspectes ou non – qui se trouvent dans les parages de cet usager, cela, à l'insu de ces personnes. Enfin, à l'étranger, l'utilisation du IMSI-catcher a permis de faire les constatations suivantes: dans certaines situations, cet appareil permet principalement d'identifier « directement » qui se trouve à un endroit déterminé ou encore de perturber le trafic téléphonique de manière ciblée. PES, JDS et droitsfondamentaux.ch se demandent, en outre, si l'utilisation de ces appareils relève réellement du code de procédure pénale. Selon le rapport explicatif, les appareils de ce type sont censés être utilisés par la police, sur ordre du ministère public, mais « dans le but de garantir la sécurité publique ». Aux yeux des trois derniers participants cités, cette tâche est une tâche de police pour laquelle la Confédération n'a aucune compétence de légiférer. Au surplus, l'art. 270ter CPP n'établit pas de critères déterminant les circonstances dans lesquelles le recours à de tels dispositifs se justifie, pas plus qu'il ne fixe, en sus de l'autorisation du tribunal des mesures de contrainte, des conditions qui doivent être réunies pour qu'une telle surveillance puisse être mise en place. Le tribunal ne peut donc se référer à aucun principe directeur lorsqu'il doit décider d'autoriser ou d'interdire une intervention au moyen desdits appareils.

TI souhaite que l'on statue expressément dans la loi que l'autorité compétente pour autoriser l'emploi de IMSI-catchers est l'OFCOM, ce qui permettra d'éviter que l'on suppose de manière erronée qu'il s'agit du tribunal des mesures de contrainte mentionné à l'al. 2. En outre, il y a lieu de préciser si l'autorisation accordée par l'OFCOM vise le recours à un certain type d'appareils ou si elle doit être requise lors de chaque intervention. NW demande, pour sa part, que la procédure d'autorisation soit réglée dans la loi.

Plusieurs participants appartenant à la branche des télécommunications[165] font observer qu'en cas d'utilisation d'IMSI-catchers, les fournisseurs de services se verront automatiquement demander de produire l'IMSI, voire le TIMSI[166] des personnes surveillées. Or la production de l'IMSI est une affaire délicate puisque l'IMSI est un élément de la sécurité du réseau de télécommunication. Tant que les organes de police procèdent eux-mêmes à la localisation d'appareils de téléphonie mobile, ils peuvent s'accommoder de cette situation. Cependant, dès qu'ils solliciteront un appui sous la forme de cartes spéciales, celui-ci coûtera très cher car il n'existe que très peu de spécialistes capables de le prêter.

MS relève que l'IMSI-Catcher permet également d'écouter les conversations. Cette fonction doit absolument être mentionnée et ressortir du titre de l'article afin d'éviter que cet appareil soit utilisé pour collecter des données aux fins visées à l'art. 269 CPP.

11.1.4 Art. 271, al. 1 et 2, CPP Protection du secret professionnel

---

[163] LU, NW, BL, SG, GL, GR, TG, VS, JU, CCDJP, CAPS.
[164] International Mobile Subscriber Identity.
[165] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
[166] Temporary International Mobile Subscriber Identity.

[1] *En cas de surveillance d'une personne appartenant à l'une des catégories professionnelles énumérées aux art. 170 à 173, l'accès direct par les autorités de poursuite pénale aux informations recueillies dans le cadre de la surveillance est empêché. Les informations qui n'ont pas de rapport avec l'objet de l'enquête ni avec le motif pour lequel la personne concernée est soumise à surveillance sont triées, sous la direction d'un tribunal. Ce tri est opéré de telle sorte que les autorités de poursuite pénale n'aient connaissance d'aucun secret professionnel.*

[2] *Le tri n'a pas lieu lorsque:*

a. des soupçons graves pèsent sur le détenteur du secret professionnel lui-même;

b. des raisons particulières l'exigent.

OW considère que la modification et l'adjonction proposées sont appropriées et correctes.

NW, BL, SG et CAPS déplorent que la disposition ne règle pas le cas de figure dans lequel le détenteur du secret professionnel est l'interlocuteur de la personne surveillée. Ils estiment qu'il faut compléter cette disposition. Lorsque le détenteur du secret professionnel fait l'objet d'une surveillance en qualité de tiers, cette surveillance devrait, selon SG et CAPS, être en outre limitée aux conversations qu'il a avec la personne suspecte (ou encore aux communications pour lesquelles la personne suspecte utilise le raccordement du détenteur du secret professionnel). Une telle limitation ne peut pas seulement être assurée par un tri, sous la direction d'un tribunal. Dans certains cas, ce tri ne pourra être opéré que moyennant des mesures techniques. Cette éventualité devrait être prévue dans la loi (celle-ci pourrait, par exemple, statuer que seules pourront être enregistrées les communications passées depuis le raccordement surveillé avec le correspondant sélectionné). Toutefois, contrairement au libellé proposé, on ne saurait exiger du tribunal qu'il ne charge pas une autorité de poursuite pénale d'évaluer les résultats de la surveillance, alors que seule une telle autorité possède le savoir-faire nécessaire à cette évaluation. Les participants précités demandent donc que l'al. 1 soit complété comme suit: « (…) l'accès direct par l'autorité de poursuite pénale *chargée de l'enquête préliminaire (…)* est empêché ».

De l'avis de FSA, l'article proposé comprend des éléments dénués de toute logique. Ainsi, on ne voit pas pourquoi les secrets professionnels seraient protégés moyennant un tri des informations figurant au dossier, lorsque ces informations n'ont pas de rapport avec l'objet de l'enquête et que le détenteur du secret professionnel est surveillé en la seule qualité d'abonné à un raccordement téléphonique et non lorsque la surveillance est ordonnée en raison de soupçons graves pesant sur le détenteur du secret professionnel. Dans les deux cas, en effet, les clients, les patients ou les créanciers ont des intérêts identiques à ce que le secret professionnel soit protégé. Il n'y a donc aucune raison de conserver dans le dossier des informations qui n'ont aucun lien avec l'objet de l'enquête et sont soumises au secret professionnel.

FSA relève que, dans tout Etat civilisé, le secret professionnel est protégé lors de l'exécution de mesures de surveillance de la correspondance par télécommunication, cela en vertu des trois principes suivants : la surveillance des installations de télécommunication des détenteurs de secrets professionnels doit rester l'exception. Ensuite, la surveillance doit être effectuée de telle sorte que seules soient enregistrées des informations qui ont un rapport avec l'objet de l'enquête. Enfin, l'évaluation des informations recueillies doit être opérée par un tribunal qui n'est pas saisi du dossier. Il résulte de ces principes que le recours à la surveillance doit rester une mesure exceptionnelle. Les informations protégées par le secret professionnel qui sont mises au jour par des tiers lors d'une surveillance doivent être retirées du dossier et ne peuvent être exploitées en justice. A la lumière de ces principes, FSA demande que la disposition soit reformulée.

11.1.5 Art. 273, al. 3, CPP Données relatives au trafic et à la facturation et identification des usagers

[3] Les données mentionnées à l'al. 1 peuvent être demandées avec effet rétroactif sur une période de douze mois au maximum, indépendamment de la durée de la surveillance.

LU, NW, CAPS et CCDJP renvoient aux considérations qu'ils ont émises à propos de l'art. 23 AP (partie III, ch. 5.4). OW estime que la modification proposée est judicieuse.

11.1.6 Art. 274, al. 4, let. c et d (nouvelles), CPP

[4] L'autorisation indique expressément:

c. si l'introduction dans un système informatique de programmes informatiques dans le but d'intercepter et de lire des données est admissible;

d. si l'utilisation par la police d'appareils permettant de déterminer les données d'identification spécifiques des appareils de téléphonie mobile et de les localiser est admissible.

OW estime que l'adjonction proposée est judicieuse.

let. c

BL et AG proposent de régler à cette lettre les modalités de l'effacement des programmes informatiques introduits dans les systèmes concernés. NW, pour sa part, souhaite que le texte règle la procédure d'autorisation applicable à l'utilisation de tels programmes.

let. d

Plusieurs participants[167] préconisent que l'expression « appareils de téléphonie mobile » soit remplacée par « moyens de communication mobile » afin que la surveillance reste admissible en cas d'utilisation de nouveaux instruments issus du progrès technologique (par exemple, notebooks équipés de cartes SIM).

CAPS et CCDJP rappellent qu'elles ont proposé de régler l'utilisation de tels appareils à l'art. 280 CPP (v. supra, partie III, ch.11.1.3, remarques concernant l'art. 270ter CPP) et préconisent, conjointement avec NW, que la procédure d'autorisation s'y rapportant soit réglée à l'art. 274 CPP.

11.1.7 Art. 278, al. 1bis, CPP Découvertes fortuites

[1bis] Si, lors d'une surveillance au sens des art. 27 et 28 de la loi fédérale du … sur la surveillance de la correspondance par poste et télécommunication, des infractions sont découvertes, les informations recueillies peuvent être utilisées aux conditions fixées aux al. 2 et 3.

OW estime que l'adjonction proposée est judicieuse.

11.2. Procédure pénale militaire du 23 mars 1979 (PPM)[168]

OW estime que les modifications et adjonctions proposées sont judicieuses et correctes.

11.2.1 Art. 70a^{bis} PPM Interception et décryptage de données *(nouveau)*

[1] Lorsque, dans le cadre d'une surveillance de la correspondance par télécommunication, les mesures de surveillance prises jusqu'alors sont restées sans succès ou lorsque les autres mesures de surveillance n'auraient aucune chance d'aboutir ou rendraient la surveillance excessivement difficile, le juge d'instruction peut ordonner,

---

167 ZH, LU, AG, GL, GR, TG, VS, JU, CCPCS, CCDJP.

168 RS 322.1

même à l'insu de la personne surveillée, l'introduction dans un système informatique de programmes informatiques permettant d'intercepter et de lire des données. Dans son ordre de surveillance, le juge d'instruction indique le type de données qu'il souhaite obtenir.

[2] L'ordre de surveillance est soumis à l'autorisation du président du Tribunal militaire de cassation.

Quelques participants[169] renvoient aux remarques qu'ils ont formulées à propos de l'art. 270[bis] CPP (v. supra, partie III, ch. 11.1.2).

11.2.2 Art. 70a[ter] PPM Utilisation de systèmes de localisation *(nouveau)*

[1] Le juge d'instruction peut ordonner l'utilisation par la police d'appareils permettant de déterminer les données d'identification spécifiques des appareils de téléphonie mobile et de les localiser. Les appareils utilisés doivent au préalable avoir fait l'objet des autorisations nécessaires.

[2] L'ordre de surveillance est soumis à l'autorisation du président du Tribunal militaire de cassation.

Plusieurs participants[170] préconisent que l'expression « appareils de téléphonie mobile » soit remplacée par « moyens de communication mobile » afin que le recours à des systèmes de localisation reste admissible en cas d'utilisation de nouveaux instruments issus du progrès technologique (par exemple, notebooks équipés de cartes SIM).

Quelques participants[171] renvoient aux remarques qu'ils ont formulées à propos de l'art. 270[ter] CPP (v. supra, partie III, ch. 11.1.3).

11.2.3 Art. 70b PPM Sauvegarde du secret professionnel

[1] En cas de surveillance d'une personne appartenant à l'une des catégories professionnelles énumérées à l'art. 75, let. b, l'accès direct par les autorités de poursuite pénale aux informations recueillies dans le cadre de la surveillance est empêché. Les informations qui n'ont pas de rapport avec l'objet de l'enquête ni avec le motif pour lequel la personne concernée est soumise à surveillance sont triées, sous la direction du président du tribunal militaire. Ce tri est opéré de telle sorte que les autorités de poursuite pénale n'aient connaissance d'aucun secret professionnel.

[2] Le tri n'a pas lieu lorsque:

a. des soupçons graves pèsent sur le détenteur du secret professionnel lui-même;

b. des raisons particulières l'exigent.

[3] En cas de surveillance d'autres personnes, les informations à propos desquelles l'une des personnes mentionnées à l'art. 75, let. b pourrait refuser de témoigner doivent être retirées du dossier de la procédure pénale et immédiatement détruites; elles ne peuvent pas être utilisées dans le cadre de cette procédure.

Pas de remarques.

11.2.4 Art. 70d, al. 3, PPM

[3] Les renseignements mentionnés à l'al. 1 peuvent être demandés avec effet rétroactif sur une période de douze mois au maximum, indépendamment de la durée de la surveillance.

Quelques participants[172] renvoient aux remarques qu'ils ont formulées à propos de la prolongation du délai de conservation prévu à l'art. 19, al. 2 AP (v. supra, partie III, ch. 4.1.2) et à l'art. 23 AP (v. supra, partie III, ch. 5.4).

11.2.5 Art. 70e, al. 4, let. c et d (nouvelles), PPM

[4] L'autorisation doit indiquer expressément :

---

169 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
170 ZH, LU, AG, GL, GR, TG, VS, JU, CCPCS, CCDJP.
171 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
172 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

c.	*si l'introduction dans un système informatique de programmes informatiques dans le but d'intercepter et de lire des données est admissible;*
d.	*si l'utilisation par la police d'appareils permettant de déterminer les données d'identification spécifiques des appareils de téléphonie mobile et de les localiser est admissible*.

S'agissant de la lettre c, quelques participants[173] renvoient aux remarques qu'ils ont formulées dans la partie III, ch. 11.1.2 à propos de l'art. 270bis CPP et s'agissant de la let. d, aux remarques formulées dans la partie III, ch.11.1.3 à propos de l'art. 270ter CPP.

11.3. Loi sur les télécommunications du 30 avril 1997 (LTC)[174]

11.3.1 Art. 6a LTC Blocage de l'accès aux services de télécommunication

Les fournisseurs de services de télécommunication doivent bloquer l'accès à la téléphonie mobile et à Internet de leurs clients n'ayant pas souscrit d'abonnement, lorsque ceux-ci ont, lors de l'ouverture de la relation commerciale, utilisé l'identité d'une personne qui n'existait pas ou qui n'a pas au préalable consenti à l'ouverture de cette relation.

Dix participants[175] se félicitent de ce que l'AP prévoie expressément le blocage obligatoire de l'accès aux services de télécommunication, en cas d'abus. Dans la pratique, on constate aujourd'hui que les délinquants qui utilisent la téléphonie mobile se servent d'appareils volés ou d'appareils pour lesquels un abonnement a été souscrit avec l'identité d'un tiers ou d'une personne qui n'existait pas. On sait par expérience que la qualité des processus de vérification de l'identité des clients, lors de la conclusion de contrats avec des opérateurs de téléphonie mobile, laisse à désirer.

OW estime que, telle que proposée, la modification de la LTC ne va pas assez loin. Seule une pratique rigoureuse d'enregistrement de chaque relation commerciale est propre à empêcher l'utilisation abusive de cartes SIM à prépaiement, constatée dans la pratique. La situation actuelle n'est pas satisfaisante pour les autorités de poursuite pénale. Cela étant, AG propose de compléter la disposition de telle sorte que les autorités de poursuite pénale puissent – éventuellement avec l'autorisation du tribunal des mesures de contrainte – ordonner un blocage de l'accès aux services de télécommunications pour les appareils utilisant des cartes Sim à prépaiement ou des cartes « wireless » à prépaiement lorsque ces cartes ont été utilisées ou continuent à être utilisées dans le but de commettre des infractions.

Orange propose de biffer purement et simplement le passage « (…) et à Internet (…) ».

---

173 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
174 RS 784.10
175 ZH, NW, CCDJP, GL, GR, TG, VS, JU, CCPCS, CAPS.