Rapport · SurPRISE

Zentrum für Technologiefolgen-Abschätzung
Centre d'évaluation des choix technologiques
Centro per la valutazione delle scelte tecnologiche
Centre for Technology Assessment

Souriez, vous êtes surveillés !

Rapport des forums de discussion sur l'utilisation des technologies modernes de surveillance en Suisse.

Réalisé dans le cadre du projet européen SurPRISE

Mars 2014

TA-SWISS

Impressum

Souriez, vous êtes surveillés !
TA-SWISS (éd.), Berne 2014
TA-P18/2014

Auteures:
Lucienne Rey et Dilini-Sylvie Jeanneret (en collaboration avec Danielle Bütschi et Christine D'Anna-Huber)

Mise en page
Helen Curty, TA-SWISS, Berne

Photos:
Nick Quine, Paris

Impression:
Jordi AG – Das Medienhaus, CH-3123 Belp

Table des matières

L’essentiel en bref

SurPRISE: ce mot pourrait s’entendre comme l’annonce d’un cadeau inattendu. En fait, c‘est l‘abréviation de «Surveillance, Privacy and Security», un projet de recherche de grande envergure financé par l’UE. Celui-ci examine le rapport problématique entre les droits fondamentaux et les technologies modernes de surveillance. Assurer la sécurité aujourd’hui, n’est-ce vraiment possible qu’au prix de moins de sphère privée? Où peut-on pour cela tabler sur d’autres idées, surprenantes peut-être?

La préoccupation centrale du projet est de savoir comment les citoyennes et ci-toyens de neuf pays d’Europe réagissent aux technologies de surveillance. Est-il vrai, comme cela est souvent insinué dans les débats politiques, que les consentent à un moins de sphère privée pour un plus de sécurité? Quelles mesures de sécurité sont-elles jugées acceptables et lesquelles pas?

Pour répondre à ces questions, plus de 1750 citoyennes et citoyens ont été interrogés, en Norvège, au Danemark, en Angleterre, en Allemagne, en Autriche, en Espagne, en Italie, en Hongrie et en Suisse, entre janvier et mars 2014, sur la manière dont ils perçoivent la relation entre surveillance, sphère privée et sécurité. En Suisse, les forums de discussion ont été organisés par le Centre d‘évaluation des choix technologiques TA-SWISS. La Suisse alémanique (Zurich), la Suisse romande (Grandson) et le Tessin (Lugano) ont chacun accueilli un forum de discussion sur une journée, qui a donné aux participantes et aux participants l‘occasion de prendre position, en groupe et lors de votes individuels, sur tout un éventail de questions liées à l‘interaction entre la sphère privée et la sécurité. Pour se préparer aux débats, ils ont reçu des informations par écrit sur trois technologies de sécurité spécifiques : la géolocalisation par GPS via le smartphone, Smart CCTV, aussi appelée vidéosurveillance «intelligente», et «Deep Packet Inspection (DPI)», autrement dit l‘analyse approfondie de données sur les utilisateurs et les applications sur Internet. Au début de chacun des trois forums, certains aspects du sujet ont été approfondis par des courts métrages documentaires.

La quintessence de tous ces entretiens entrera dans des recommandations qui seront soumises aux parlements des pays participants et à la Commission de l’UE. Le but de SurPRISE est ainsi de contribuer à un débat public et politique mieux informé. Et de veiller à ce que l’opinion de la population européenne joue à cet égard le rôle qui lui revient.

Importance de la protection des données en Suisse

Lors des forums de discussion en Suisse, il est apparu que la protection des données est une revendication centrale des citoyennes et des citoyens. Dans chacune des trois régions linguistiques qui ont pris part au projet SurPRISE, l‘éventualité qu‘on puisse perdre le contrôle sur les propres données a été un sujet de préoccupation évoqué. Les résultats du projet SurPRISE soulignent le fait que, de l‘avis de participantes et des participants, les technologies de surveillance ne devraient être utilisées que dans un cadre clairement défini sur le plan légal. Il conviendrait également de faire savoir quelles informations sont collectées, qui en assume la responsabilité et quels sont les buts poursuivis.

En Suisse plus qu‘ailleurs, un sentiment de sécurité prévaut. Les mesures de surveillance sont de ce fait perçues avec d‘autant plus de scepticisme. Leur utilisation de routine bute dans notre pays contre des réserves plus marquées que la moyenne des pays participant à SurPRISE. Il s‘avère également que les habitantes et les habitants de la Suisse attachent beaucoup d‘importance à la sphère privée. Ils font preuve d‘un scepticisme vis-à-vis de l‘utilisation régulière de technologies de surveillance par l‘Etat supérieur à la moyenne des pays participants, et ce, même

si les autorités jouissent en Suisse d‘un capital confiance comparativement élevé.

De ce point de vue, les Suissesses et les Suisses attachent une importance accrue à la protection de la sphère privée et des données personnelles qu‘à la prévention de menaces criminelles et terroristes, d‘autant que de nombreuses personnes émettent des doutes quant à la capacité de la technique à fournir des instruments adéquats pour améliorer réellement la sécurité nationale.

Une protection des données forte et dotée des moyens requis compte parmi les revendications récurrentes et exprimées avec insistance dans le cadre de SurPRISE.

1. SurPRISE: contexte et réalisation

Depuis que l'ancien collaborateur du renseignement américain Edward Snowden a révélé, à la stupéfaction du grand public, que les données de tout un chacun étaient espionnées à grande échelle par les services de sécurité des Etats-Unis, les nerds passionnés d'informatique ne sont plus seuls à s'intéresser à ce qui se passe dans les coulisses d'internet et des communications électroniques. D'où le nombre important de personnes qui se sont annoncées auprès de du Centre d'évaluation des choix technologiques TA-SWISS après que celui-ci ait lancé une invitation à trois forums de discussion sur le difficile équilibre entre la protection de la sphère privée et le recours à des technologies de surveillance aux fins de protéger la sécurité nationale et de combattre la criminalité. Chacun de ces débats a porté sur deux technologies de surveillance ; l'inspection approfondie des paquets (ou DPI pour Deep Packet Inspection), qui permet d'espionner les données de connexion et les contenus des communications électroniques, et la géolocalisation de personnes par le biais de leurs téléphones portables. La surveillance étatique, autrement dit le recours par les autorités à des techniques visant à préserver la sécurité nationale, était au cœur des débats. Les participantes et les participants étaient toutefois libres de quitter ce cadre, et ils ont également abordé, au fil des discussions, l'utilisation des technologies de surveillance à des fins privées ou économiques.

Ces forums de discussion de TA-SWISS s'incrivaient dans un vaste projet international mené dans le cadre de l'Union européenne. Au total, neuf pays – en plus de la Suisse, également l'Allemagne, l'Autriche, le Danemark, l'Espagne, la Grande-Bretagne, la Hongrie, l'Italie et la Norvège – ont participé à ce projet appelé SurPRISE, acronyme de «Surveillance, Privacy and Security». Les partenaires du projet ont élaboré en commun le cadre théorique, les hypothèses de travail et le design méthodologique. Celui-ci comprenait à la fois des éléments quantitatifs et qualitatifs. des technologies du DPI et de la géolocalisation des smartphones, traitées en Suisse, le projet a abordé aussi la vidéosurveillance intelligente ; chaque pays participant pouvait choisir les deux technologies qu'il souhaitait mettre en discussion.

En Suisse, les modalités de réalisation de SurPRISE ont été particulièrement exigeantes. Car à la différence des autres partenaires du projet, qui n'ont organisé chacun qu'un seul forum de discussion, la Suisse en a mis trois sur pied, un dans chacune des trois régions linguistiques du pays – la Suisse alémanique, romande et italienne.

Un nombre surprenant de personnes se sont inscrites auprès de TA-SWISS pour participer à SurPRISE ; parmi plus de mille intéressés, TA-SWISS a sélectionné trois groupes composés chacun d'une centaine de participantes et participants. Les forums de discussion devaient regrouper des femmes et des hommes de toutes les classes d'âge et d'horizons professionnels différents. Pour se préparer, les personnes sélectionnés ont reçu une brochure d'information sur les technologies mises en discussion. Les débats se sont déroulés par tables, qui ont regroupé chacune de six à huit participantes et participants ainsi qu'une facilitatrice ou un facilitateur.

Toutes les rencontres ont suivi le même schéma, que ce soit en Suisse ou dans autres les pays partenaires. Après un mot de bienvenue par les organisateurs locaux, les participantes et participants étaient instruits sur le fonctionnement de leurs cliqueurs. Ces petits appareils servaient à répondre aux questions à choix multiple qui ont fourni les résultats quantitatifs de SurPRISE. Après s'être tous familiarisés avec les cliqueurs, les participantes et participants répondaient à une première série de questions. Un film d'information de cinq minutes environ sur le DPI lançait ensuite les discussions , d'une durée d'à peu près

quarante-cinq minutes. Deux tables comptaient également une collaboratrice de TA-SWISS qui prenait des notes détaillées des discussions; ces transcriptions ont servi de base pour l'analyse qualitative des arguments des participantes et participants. Après ces discussions, les groupes échangeaient brièvement, en plenum, leurs principales conclusions. La deuxième partie de la journée, après le repas de midi, portait sur la géolocalisation des smartphones et suivait pour l'essentiel le même schéma. Quelques questions générales ayant trait à l'attitude à l'égard des technol-ogies de sûreté ont été posées deux fois – une fois au début et une fois à la fin de l'évènement. Ceci a permis de constater si les connaissances acquises pendant la journée avaient conduit à des changements d'opinions. La rencontre se terminait par une discussion de quarante-cinq minutes environ qui visait à formuler des recommandations pour les politiciens et autres décideurs au sujet de l'utilisation de technologies de surveillance.

Les participantes et participants ont eu l'occasion de faire part des préoccupations qui leur tenait à cœur, en se servant pour cela de «cartes postales» préimprimées qui leur avaient été distribuées. L'évaluation qui suit tient compte de ces cartes postales lorsqu'elles comprennent des arguments qui n'ont pas déjà été avancés pendant les discussions.

1.1. Résultats empiriques des discussions animés

Les trois forums de discussion suisses – en Suisse allemande à Zurich, en Suisse romande à Grandson, et au Tessin à Lugano – se sont déroulés dans une atmosphère agréable et collégiale. Les participantes et participants de Suisse romande, en comparaison de celles et ceux des autres régions linguistiques, - ont posé davantage de questions et ont en outre – comme les personnes de Lugano – fait un large usage des cartes postales à leur disposition pour faire part de leurs remarques personnelles et apporter des compléments.
A Zurich et Grandson, TA-SWISS a constaté avec plaisir que la plupart des personnes inscrites à SurPRISE ont effectivement participé à l'événement : à Zurich, 88 étaient présentes sur 103 annoncées, à Grandson 90 sur 105. A Lugano, par contre, la proportion des absents a été un peu plus grande, peut-être en raison du temps printanier et ensoleillé qui régnait ce jour là. Seulement 75 sur 103 personnes ont pris le chemin de l'Aula Magna de l'Université du Tessin.

En comparaison des autres pays participants au projet SurPRISE, les trois forums de discussion suisses se sont caractérisés par une plus forte présence de personnes jouissant d'un niveau d'éducation élevé. En conséquence, les professionnels occupant des postes de cadres supérieurs étaient surreprésentés. Il en allait de même de personnes bien formées, ce qui correspond de nouveau à des activités professionnelles exigeantes.

Avec 5 % de personnes de 18 à 29 ans, et 10 % de 30 à 39 ans, les jeunes étaient nettement sous-représentés parmi les participants et participantes suisses (ces chiffres étaient de respectivement 17 et 14 % en moyenne pour l'ensemble des pays ayant participé au projet SurPRISE). Ce déséquilibre a été remarqué dans tous les forums de discussion et en partie critiqué : «Il est regrettable que les 18 à 30 ans soient sous-représentés. Le résultat de la discussion aurait certainement été tout à fait différent auprès des jeunes», a relevé quelqu'un à Zurich. Des commentaires similaires ont aussi été faits à Lugano et à Grandson. Pour tenir compte de ce problème de l'échantillon, les résultats ont été en partie évalués par groupes d'âge – notamment en ce qui concerne les questions touchant à la protection de la sphère privée, particulièrement importantes pour le projet. De plus, une évaluation en fonction de l'âge a été effectuée sur toutes

les séries de données des autres pays participant à SurPRISE, afin de vérifier si des différences existent bel et bien entre les générations. Les résultats ne sont pas faciles à interpréter ; néanmoins, ils ne permettent nullement de déduire que la jeune génération accorderait en général moins d'importance à la sphère privée ou envisagerait les questions de sécurité différemment. C'est ainsi que 62 % des 18 à 29 ans approuvent l'affirmation selon laquelle les technologies de sécurité portent atteinte à la vie privée en général (29 % sont «tout à fait d'accord», 33 % «d'accord» avec cela). Ils sont 70 % dans la catégorie des 30 à 39 ans (42 % «tout à fait d'accord», 28 % «d'accord»), et dans celle des 40 à 49 ans, 63 % sont inquiets pour la sphère privée (33 % «tout à fait d'accord», 30 % «d'accord»). On ne saurait affirmer que cette préoccupation croît avec l'âge, car dans la classe des 50 à 59 ans, 62 % se font du souci pour la protection de la sphère privée, dans celle des 60 à 69 ans 65 %, et dans celle des 70 ans et plus 55 %. Les différences constatées entre les groupes d'âge ne sont pas faciles à interpréter, d'autant plus qu'elles ne varient que de quelques unités. Les évaluations en fonction de l'âge pour l'échantillon transnational de SurPRISE (au total 1773 personnes) permettent de conclure que si davantage de jeunes avaient participé en Suisse, les résultats ne divergeraient pas systématiquement de ceux disponibles actuellement.

Le panel suisse représente sous un autre rapport encore un «cas particulier»: alors que la proportion des indigènes s'élève à presque 89 % en moyenne pour l'ensemble des pays prenant part au projet, elle est à peine de 79 % en Suisse ; dans les parties francophones et italophones du pays notamment, de nombreuses personnes titulaires d'un passeport étranger ont participé à SurPRISE ; la différence entre régions linguistiques quant à la présence de citoyens qui ne sont pas de nationalité suisse est statistiquement significative. Il s'agissait le plus souvent de personnes ayant une double nationalité de deux pays européens (10 %) ; en seconde position venaient celles jouissant à la fois de la citoyenneté d'un Etat européen et de celle d'un Etat non européen. Ces chiffres correspondent à la composition démographique de la population résidant en Suisse, qui comptait à fin 2012, selon l'Office fédéral de la statistique, 24 % de ressortissants étrangers.

La proportion entre hommes et femmes présentait une légère surreprésentation masculine. La composition du groupe de Grandson, qui comprenait 55 % d'hommes et 44 % de femmes (quelques personnes n'ont pas répondu à cette question), était la plus équilibrée. En revanche, les groupes reflétaient bien la diversité des branches professionnelles – du secteur de l'administration et de la vente à celui de l'agriculture et de l'économie forestière, en passant par les professions techniques ; toutefois, la forte présence de fonctions de cadres était de nouveau manifeste.

Dans la suite du texte, si la significativité statistique n'est pas expressément mentionnée dans le commentaire des différences établies, il faut considérer qu'elle n'est pas atteinte et qu'il n'est pas exclu que ces différences soient alors dues au hasard.)

	Participants dans toute la Suisse *N=254*	Participants de Zürich *N=88*	Participants de Grandson *N=91*	Participants de Lugano *N=75*
Total	254	88	91	75
Age				
18-29	5	4	5	5
30-39	10	13	11	4
40-49	25	24	25	25
50-59	27	25	27	29
60-69	25	25	20	29
70+	6	5	8	6
Sans réponse	1	1	1	0
Sexe				
féminin	41	39	43	40
masculin	57	58	55	59
Sans réponse	1	2	2	1
Education				
École primaire	1	0	2	0
École secondaire I	2	2	1	2
École secondaire II	6	3	4	10
Qualification professionnelle	20	17	15	31
Université-HES (premier cycle)	37	50	30	29
Université-HES (postgrades)	32	23	45	25
sans réponse	1	2	1	0
Lieu d'habitation				
Zone métropolitaine	11	17	16	0
Région urbaine	41	38	41	47
Région rurale	45	45	41	51
Sans réponse	1	0	2	1
Enfants âgés de moins de 16 ans				
oui	29	29	29	29
non	41	68	68	70
Sans réponse	1	2	2	1

Figure 1: Socio-démographie des participants (pourcentage)

2. La Suisse, havre de sécurité

La manière selon laquelle le grand public perçoit et juge les technologies de sécurité dépend largement de la question de savoir si les gens se sentent protégés sur leur lieu de domicile et dans leur vie quotidienne. Plusieurs points du questionnaire de SurPRISE s'intéressaient à connaître le sentiment de sécurité personnelle des participantes et participants.

Il est apparu qu'en majorité, la population résidant en Suisse se sent sûre voire même très sûre. En effet, environ 85 % des participantes et participants ont approuvé l'affirmation selon laquelle ils se sentent généralement en sécurité dans leur vie quotidienne (contre environ 79 % en moyenne de tous les pays) ; un petit tiers s'est placé dans la catégorie la plus élevée correspondant à un fort sentiment de sécurité, en choisissant «tout à fait d'accord» en réponse à cette affirmation. Seuls le Danemark et la Norvège ont atteint dans cette catégorie des valeurs supérieures à la Suisse. Une question formulée de façon un peu plus ciblée, portant sur le niveau de sécurité de la Suisse, a confirmé ce résultat : alors qu'en moyenne de tous les pays du projet SurPRISE, 66 % des participantes et participants ont adhéré à l'affirmation selon laquelle ils vivent dans un pays sûr, en Suisse 85 % ont répondu affirmativement à cette question (40 % se sont déclarés «tout à fait d'accord» et 45 % ont approuvé sans plus).

Il existe cependant des différences significatives entre les trois groupes de discussion suisses. Dans l'ensemble toutefois, elles confirment la tendance d'un sentiment de sécurité élevé. Le taux d'approbation le plus fort , à savoir 93 %, a été relevé à Zurich (38 % sont «tout à fait d'accord» avec l'affirmation selon laquelle ils se sentent en sécurité dans leur vie quotidienne, et 56 % «d'accord» avec la même affirmation). A Grandson, 82 % ont souscrit à l'affirmation selon laquelle ils se sentent généralement en sécurité dans leur vie quotidienne ; mais ici aussi, la catégorie des personnes qui rejoignent avec force cette affirmation obtient un score moins élevé (30 %) que celle des personnes qui ne font que l'approuver (52 %). C'est à Lugano, manifestement, que l'on se sent le moins en sécurité, où néanmoins 77 % ont confirmé se sentir généra-

	N	Tout à fait d'accord	D'accord	Ni d'accord ni pas d'accord	Pas d'accord	Pas du tout d'accord	SA	Total
		Pourcentage						
"Je me sens généralement en sécurité dans ma vie quotidienne"	*251*	28	57	11	3	1	0	100
"J'estime que ce pays est un endroit où l'on vit en sécurité"	*251*	40	45	12	3	0	0	100

Figure 2: Attitudes générales sur la sécurité en Suisse

	N	Tout à fait d'accord	D'accord	Ni d'accord ni pas d'accord	Pas d'accord	Pas du tout d'accord	SA	Total
		Pourcentage						
"Je me sens généralement en sécurité dans ma vie quotidienne"	*86*	38	56	2	3	1	0	100
"J'estime que ce pays est un endroit où l'on vit en sécurité"	*87*	44	46	7	2	1	0	100

Figure 3: Attitudes générales sur la sécurité pour la Suisse alémanique

lement en sécurité leur vie quotidienne : 16 % seulement ont approuvé sans réserve («tout à fait d'accord») et 61 % ont répondu affirmativement à la question («d'accord»). Mais lorsque la question est formulée de façon spécifique en référence à la Suisse (« la Suisse est un pays où l'on vit en sécurité »), les réponses atteignent au Tessin aussi un taux d'approbation élevé, de 84 % (40 % de «tout à fait d'accord», 44 % de «d'accord»).

Dans les données de SurPRISE provenant des pays environnants, on retrouve un modèle nord-sud similaire à celui qui apparaît au niveau suisse. Les participantes et les participants d'Italie ont en effet exprimé un sentiment de sécurité bien moindre si on le compare en particulier à celui qui prévaut dans les pays nordiques et en Allemagne : dans leur vie quotidienne, 38 % des Italiennes et des Italiens se sentent en sécurité, tandis que pour 23 % d'entre eux, c'est plutôt le sentiment d'être menacé qui domine. En comparaison, les chiffres en Allemagne sont de 66 %, respectivement 1 %.De nombreuses affirmations faites pendant les discussions démontrent que la Suisse est effectivement considérée comme un havre de sécurité. On oppose volontiers la situation qui règne dans ce pays à celle perçue ou supposée ailleurs : «Je fais confiance à notre société et à nos politiciens. Mais si je me trouvais au Pakistan, je verrais peut-être les choses autrement», a estimé une des personnes, alors qu'une autre a relevé : «En Suisse, avec le gouvernement actuel, je me sens en sécurité. D'autre part, la technique de surveillance permet de trouver rapidement les détracteurs du système. Cela fait du souci, même lorsqu'on n'est pas concerné». Une autre personne argumente de façon similaire : «Je ne me fais aucun souci quant à ce que je dis ouvertement. Mais dans des pays totalitaires, cela peut être énormément exploité. C'est là mon problème principal. Pas que n'importe qui puisse trouver quelque chose à mon sujet».

	N	Tout à fait d'accord	D'accord	Ni d'accord ni pas d'accord	Pas d'accord	Pas du tout d'accord	SA	Total
		Pourcentage						
"Je me sens généralement en sécurité dans ma vie quotidienne"	*90*	30	52	12	3	3	0	100
"J'estime que ce pays est un endroit où l'on vit en sécurité"	*90*	37	43	13	7	0	0	100

Figure 4: Attitudes générales sur la sécurité pour la Suisse romande

	N	Tout à fait d'accord	D'accord	Ni d'accord ni pas d'accord	Pas d'accord	Pas du tout d'accord	SA	Total
		Pourcentage						
"Je me sens généralement en sécurité dans ma vie quotidienne"	*75*	*16*	61	19	4	0	0	100
"J'estime que ce pays est un endroit où l'on vit en sécurité"	*75*	40	44	16	0	0	0	100

Figure 5: Attitudes générales sur la sécurité au Tessin

3. La surveillance suscite des réserves dans notre pays

Qui se croit en sécurité dans son propre pays est manifestement plutôt sceptique vis-à-vis de la surveillance par l'Etat. Cette conclusion s'impose en tout cas au vu des données quantitatives de SurPRISE. Ainsi se confirme l'une des principales hypothèses que les partenaires internationaux du projet ont développées lors de la préparation des forums de discussion(voir à ce sujet aussi 2.8) 38 % des participantes et participants suisses étaient d'avis qu'il faut systématiquement recourir à des technologies de surveillance pour améliorer la sécurité nationale, tandis que 42 % se disaient opposés à une telle utilisation. Près de 20 % étaient indécis. Les participantes et participants suisses sont ainsi nettement plus réservés que la moyenne des pays partenaires de SurPRISE. En moyenne globale, un peu plus de la moitié (exactement 54 %) se sont prononcés pour le recours systématique à des technologies de surveillance, alors que le résultat de ses opposants atteignait tout juste 26 %.

Le fait que le sentiment de sécurité personnelle va de pair avec le rejet de techniques de surveillance se confirme aussi au vu de résultats au niveau suisse. Le recours à des techniques de surveillance a obtenu le plus d'avis favorables au Tessin, où les habitantes et habitants se sentent de façon générale le moins sûrs. Ici, l'affirmation selon laquelle des technologies de surveillance devraient être utilisées systématiquement pour renforcer la sécurité nationale a recueilli un peu plus de 56 % des suffrages. En Suisse romande, cette assertion n'a trouvé qu'à peine 32 % de partisans, tandis qu'elle atteint un score de 29 % en Suisse alémanique, où la sécurité subjective obtient la meilleure note. Ces différences entre régions linguistiques sont statistiquement significatives.

L'argument selon lequel celui qui n'a rien fait de mal n'a pas à s'inquiéter des technologies de surveillance est également écarté en Suisse : 64 % l'ont rejeté, contre 51 % en moyenne de tous les pays. Sur ce sujet aussi, la structure des opinions à l'intérieur de la Suisse coïncide avec celle de l'évaluation subjective du sentiment de sécurité : ce raisonnement a été écarté le plus fortement en Suisse alémanique, par 83 % des voix ; la Suisse romande suit avec un score de presque 66 % ; vient enfin la Suisse italienne avec 40 %. Ces différences sont statistiquement significatives.

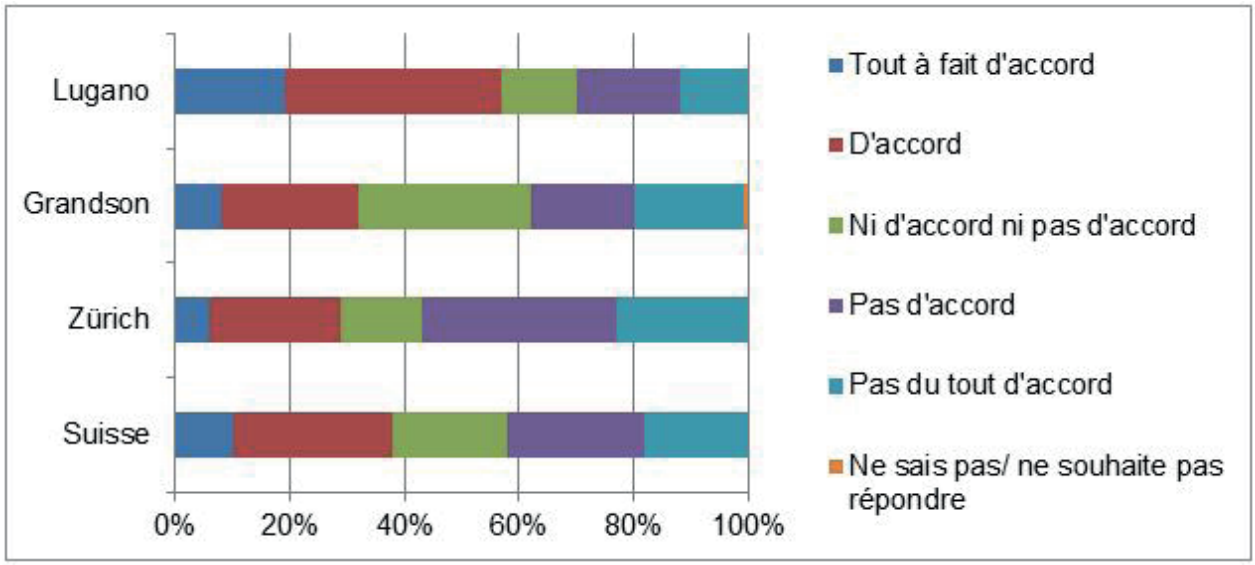

Figure 6: «Dans l'ensemble, je crois que les technologies de sécurité basées sur la surveillance devraient systématiquement être utilisées pour améliorer la sécurité nationale.»

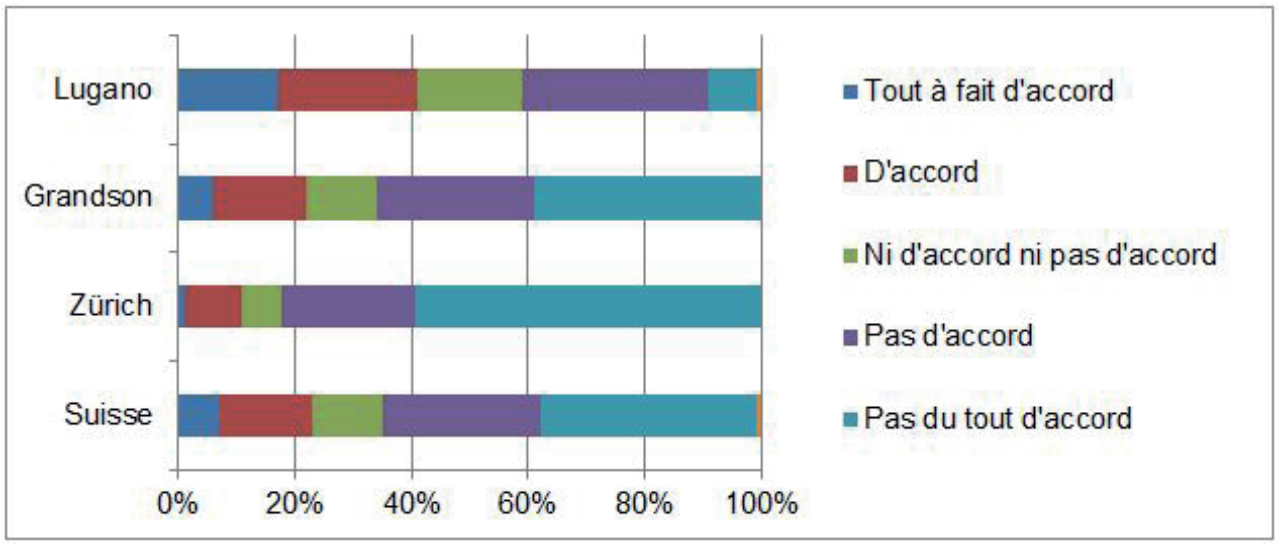

Figure 7: «On n'a pas à s'inquiéter des technologies de sécurité basées sur la surveillance si on ne fait rien de mal.»

Les participantes et participants suisses se montrent plus sceptiques que les citoyennes et citoyens d'autres pays aussi quand il s'agit d'apprécier en général les risques d'abus en lien avec les technologies de surveillance.

En effet, en Suisse, un peu plus de 80 % sont d'accord avec l'affirmation selon laquelle il est probable que les technologies de sécurité, une fois mises en place, soient utilisées de manière abusive (36 % «tout à fait d'accord», 45 % «d'accord» sans plus).

En moyenne de tous les pays, seulement 70 % sont d'accord avec cette affirmation (35 % tout à fait, 35 % simplement d'accord). De plus, des différences statistiquement significatives sont attestées à l'intérieur de la Suisse à propos de cette question.

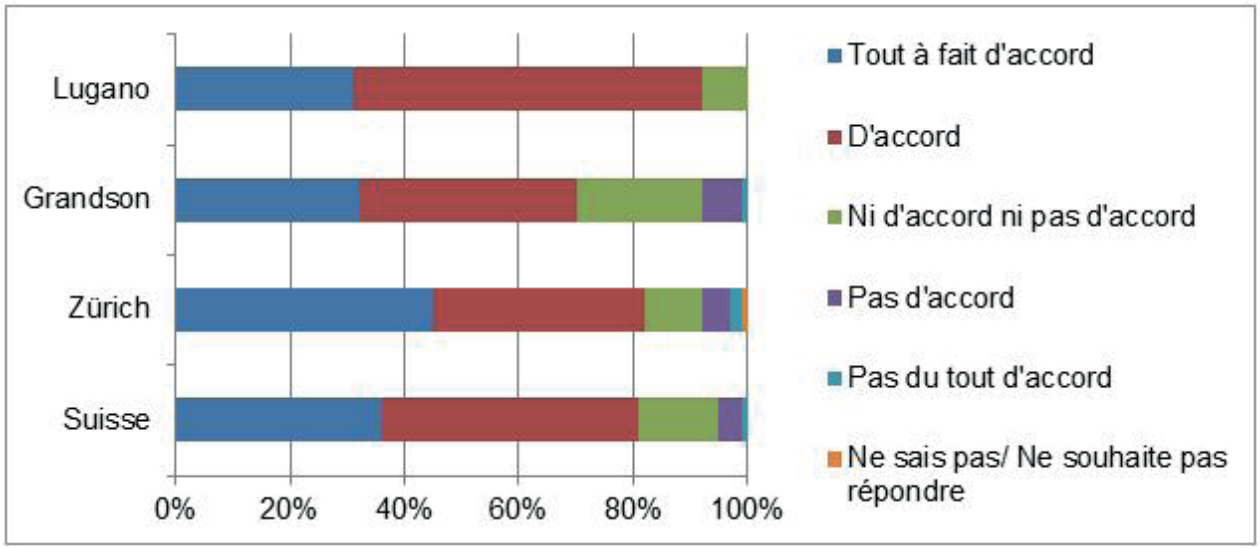

Figure 8: «Une fois les technologies de sécurité basées sur la surveillance mises en place, il est probable qu'elles soient utilisées de manière abusive.»

Avec un taux d'approbation de 92 %, le Tessin est particulièrement sceptique (31 % souscrivent avec insistance à cette affirmation, 61 % sans renchérir). La Suisse alémanique se place dans la moyenne suisse avec au total 82 % (45 % sont tout à fait d'accord, 37 % d'accord), tandis que la Suisse romande est la moins pessimiste avec un total de 70 % (32 % tout à fait d'accord, 38 d'accord sans plus).

Différentes prises de position révèlent l'ambivalence de l'attitude à l'égard des technologies de surveillance «Jusqu'à maintenant, j'ai fait confiance aux technologies et à leur utilisation. Mais avec ces nouvelles technologies, je me rends compte que je n'ai pas de motifs suffisants pour faire confiance. Notamment, parce que je ne maîtrise rien de la récolte et de l'utilisation de mes données», a dit une des personnes. Et une autre de renchérir : «La technologie n'est pas la meilleure solution pour augmenter la sécurité. Plutôt répartir la richesse et l'éducation. Il est plus bénéfique d'investir en peace building qu'en sécurité.» Des déclarations, semblables en substance, figurent sur des cartes postales de tous les groupes de discussion.

Alors que dans notre pays, les participantes et les participants se sentent plutôt moins menacés par des dangers dans leur vie quotidienne que les habitantes et habitants d'autres pays européens, ils se font tendanciellement plus de souci de sécurité quand ils naviguent sur l'internet. En Suisse, plus de 66 % déclarent se soucier de sécurité quand ils sont en ligne.

4. L'internet comme porte ouverte sur un monde menaçant

En moyenne de tous les pays participants, la proportion de personnes inquiètes pour leur sécurité s'élève à un peu moins de 62 %. En caricaturant un peu, on peut dire que l'internet passe aux yeux des Confédérés comme une porte ouverte par laquelle toutes sortes de dangers peuvent accéder à l'idylle nationale. Cette vision des choses a d'autant plus de poids que les Suissesses et les Suisses sont manifestement très fréquemment en ligne : 94 % des participants ont déclaré être connectés souvent ou même en permanence à l'internet. La moyenne sur tous les pays membres de SurPRISE atteint 88 %. A l'inverse, seulement 3 % des participants suisses ont indiqué n'être que rarement ou même jamais en ligne, contre 5 % en moyenne pour tous les pays. Les résultats du projet SurPRISE correspondent ainsi au constat du World Internet Project (WIP). Le rapport de 2012 montre que la Suisse fait partie des pays qui utilis le plus internet. Alors qu'en Italie ce sont 51%, en Espagne 68 % et au Royaume-Uni 70 % de la population qui surfent sur Internet en Suisse ce taux est de 77 %, ce qui est un taux plus élevé que dans les autres pays qui ont été étudiés dans le cadre de WIP en 2012 et qui ont participé à SurPRISE.

Le degré de préoccupation relative à la sécurité sur internet n'est pas partout le même en Suisse : c'est en Suisse romande qu'il semble être le plus prononcé : 40 % sont d'accord avec l'affirmation selon laquelle ils sont très soucieux quand ils naviguent sur le web (et 27 % reconnaissent qu'ils sont soucieux). Au Tessin aussi, surfer en toute ingénuité est plutôt l'exception, car 32 % se disent très soucieux et 48 % soucieux. En comparaison, on semble voir la situation de façon plus détendue en Suisse alémanique, où la proportion des personnes très inquiètes atteint 18 % et de celles simplement inquiètes 37 %. Ces différences sont statistiquement significatives.

De manière générale, selon les déclarations des participantes et participants au sujet des technologies de sécurité ou de l'internet, les divers aspects de la globalisation des échanges et des communications semblent être perçus comme un problème plutôt que comme un avantage ; selon les avis exprimés, la globalité de l'internet est synonyme de confusion, de compréhension difficile et d'une réglementation impossible : «C›est aussi inquiétant que ce soit global; les lois nationales ne s›appliquent pas», relève par exemple une des personnes à propos du DPI.

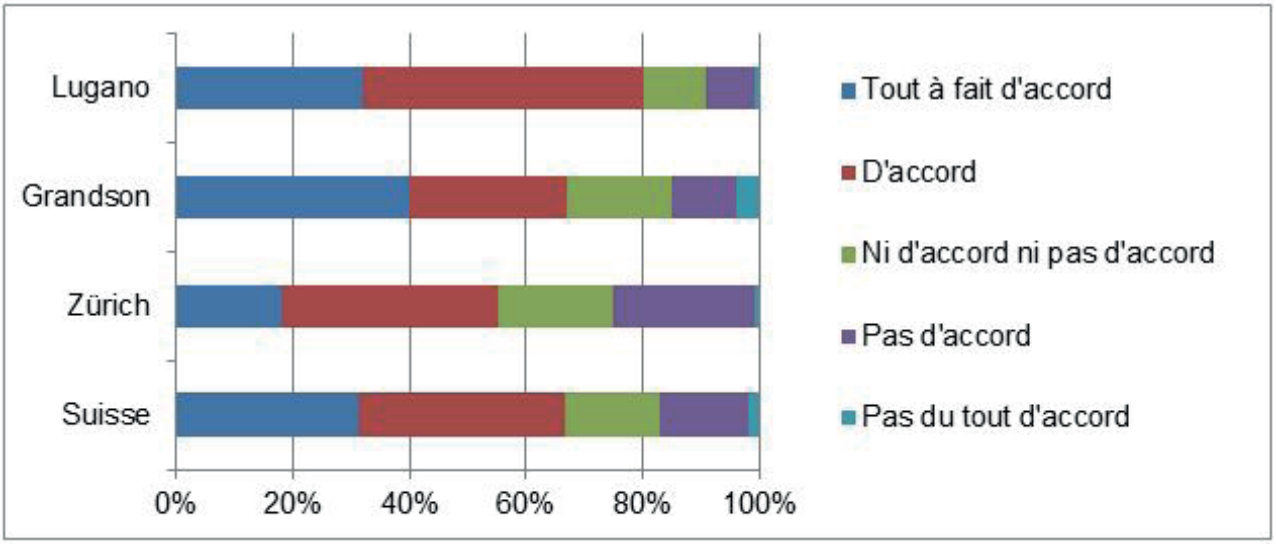

Figure 9: «Je me soucie de sécurité, quand je suis en ligne.»

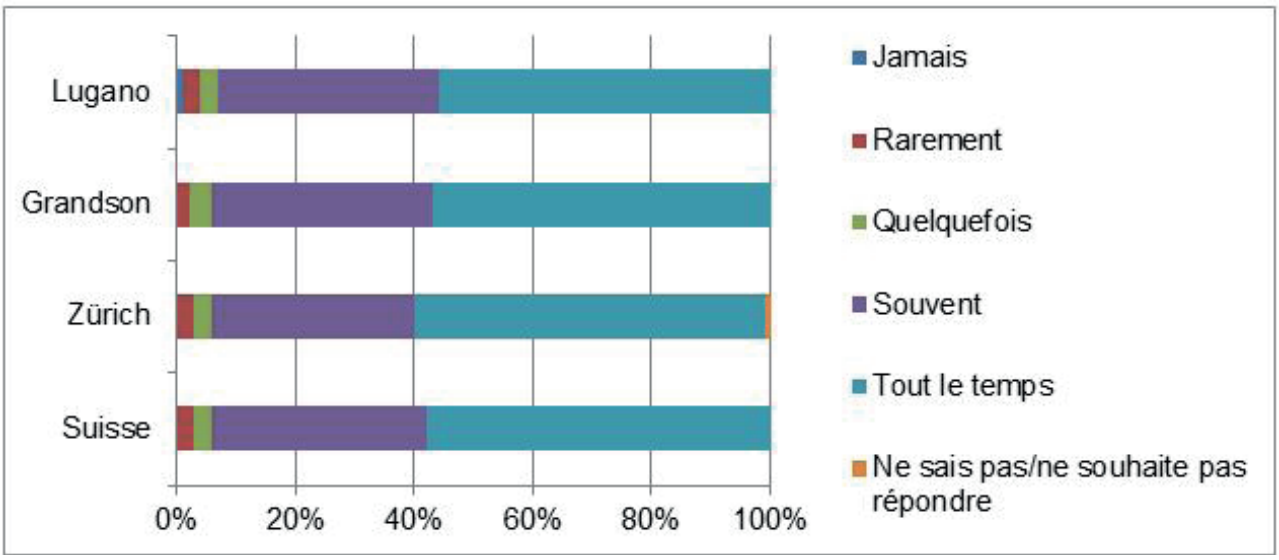

Figure 10: «A quel rythme utilisez-vous l'internet ?»

«Ailleurs le problème est certainement plus grand que chez nous», retient une autre en rapport avec la réglementation d'applications recourant à la géolocalisation. A Zurich enfin, quelqu'un est convaincu d'une chose. «La démocratie ne fonctionne que là où les gens pensent à peu près la même chose. Dans d'autres cultures, nous avons des définitions tout à fait différentes».

4.1. Le point de vue générationnel sur la vie privée sur l'Internet

Pendant les forums de discussion, et aussi dans les remarques écrites, sur les «cartes postales», des participantes et participants se sont plaints de la sous-représentation des «digital natives»; des jeunes gens qui ont grandi avec Facebook et Cie seraient beaucoup plus insouciants ou attribueraient plus de valeur aux avantages des réseaux sociaux qu'à la protection de leurs données. «Il serait passionnant de connaître l'expression des opinions en fonction de l'âge. Que pensent les teens et les twens de cette technique ? Ma belle-fille aime la pub à droite sur Facebook. Elle aime les offres spéciales», a constaté quelqu'un, et une autre personne a observé : «J'ai deux filles, de seize et dix ans. Pour elles, cette technologie est normale, elles se fichent des dangers». C'est pourquoi TA-SWISS a évalué une série de questions par groupes d'âge – notamment celles qui ont trait à l'attitude à l'égard de la sécurité personnelle et de la sphère privée.

Une première chose que l'on constate à ce niveau est que les jeunes n'utilisent pas internet de façon plus insouciante que le reste de la population. Dans la tranche de 18 à 29 ans, 69 % ont répondu affirmativement à la question de savoir s'ils se préoccupent de sécurité quand ils naviguent sur le web (53 % sont même «tout à fait d'accord» avec l'affirmation correspondante). Ce résultat est même un peu au-dessus de la moyenne suisse de 67 %.

Mais vu que dans l'ensemble de l'échantillon suisse, seulement treize participantes et participants avaient moins de 29 ans, des raisons statistiques imposent de regrouper les classes d'âge et de calculer les valeurs pour les personnes de 18 à 39 ans. Dans ce cas, ils ont été encore 63 % à confirmer qu'ils se soucient de sécurité quand ils sont sur le web (dont 37 % adhèrent pleinement à cette affirmation en se disant «tout

à fait d'accord» et 26 % se disent simplement «d'accord»). Ils se situent ainsi un peu au-dessous de la moyenne suisse et pratiquement au même niveau que le groupe d'âge des 40 à 59 ans (63 %). Un point intéressant est le fait qu'une petite minorité seulement navigue sur le web sans se faire aucun souci : seulement 13 % des 18 à 39 ans ont rejeté l'affirmation selon laquelle ils se soucieraient de sécurité quand ils sont en ligne ; cependant, personne dans cette classe d'âge n'a renchéri sur ce rejet. Sur ce point, 13 % des 40 à 59 ans ont répondu négativement, 5 % même très négativement.

En fait, ce n'est qu'à l'âge de la retraite que les réserves à l'égard de la navigation sur le web augmentent substantiellement – en effet, 77 % des plus de 60 ans s'inquiètent de sécurité lorsqu'ils sont en ligne (39 % approuvent tout à fait l'affirmation correspondante, 37 % l'approuvent simplement).

4.2 La sphère privée – un idéal qui reste d'actualité

De l'avis des participantes et participants suisses, la sphère privée a une grande importance. Au tout début de la journée, 30 % des participantes et participants se sont déclarés tout à fait d'accord avec l'affirmation selon laquelle ils craignent que les technologies de sécurité portent atteinte à leur vie privée ; 36 % d'autres étaient simplement d'accord. Avec ce total de 66 %, la Suisse est au-dessus de la moyenne de 57 % de l'ensemble des pays participants. Symétriquement, la préoccupation des Suissesses et des Suisses pour la sphère privée se confirme au travers de la négation de l'affirmation : 12 % l'ont rejetée, 2 % même de façon catégorique. Avec un total de 14 % de voix négatives, la Suisse atteint sous ce rapport un score inférieur à la moyenne de tous les pays participants, égale à 23 % ; en d'autres termes, en moyenne de tous les pays participants, une plus grande proportion de personnes estime que la sphère privée n'est pas menacée.

Au cours de la journée de SurPRISE, les craintes au sujet de la protection de la sphère privée ont encore un peu augmenté. En Suisse, après que les participantes et participants aient vu les vidéos sur le DPI et la géolocalisation par le téléphone portable et discuté à ce sujet, 70 % de ces personnes ont souscrit à l'affirmation selon laquelle les technologies de surveillance peuvent porter atteinte à la vie privée en général (contre 67 % en moyenne de tous les pays).

Un point intéressant est que les craintes fondamentales touchant aux atteintes de la vie privée

	N= 245	Tout à fait d'accord	D'accord	Ni d'accord ni pas d'accord	Pas d'accord	Pas du tout d'accord	Total
		Pourcentage					
18-39 ans	*38*	37	26	23	13	0	100
40-59 ans	*128*	23	40	19	13	5	100
Plus de 60	*77*	39	37	6	17	0	100
Ne souhaite pas répondre	*2*	50	0	50	0	0	100

Figure 11: «Quand je suis en ligne, je me soucie de sécurité.»

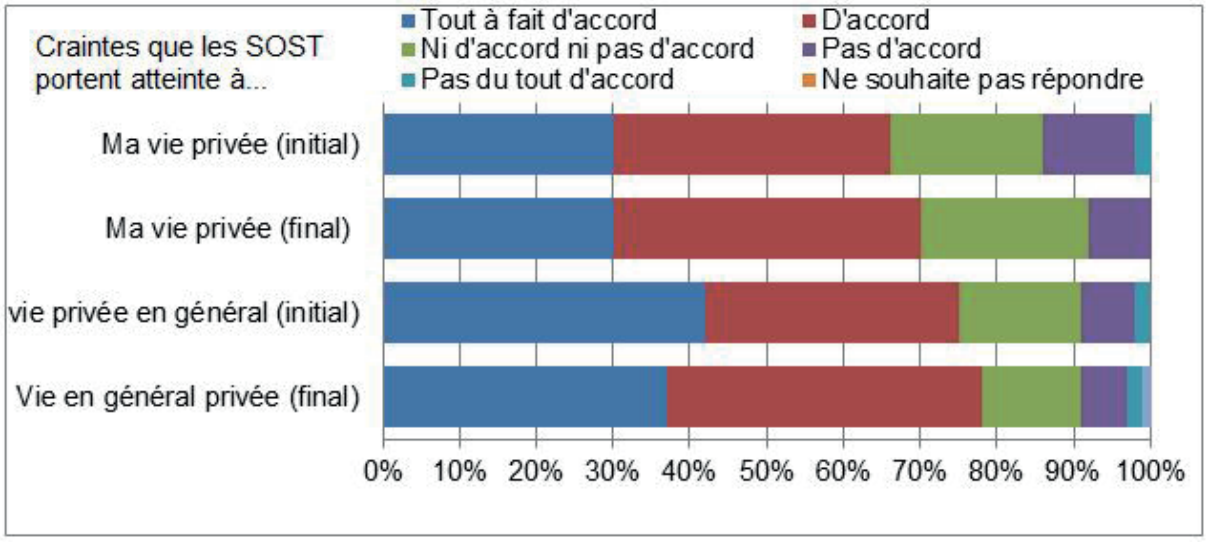

Figure 12: Inquiétudes pour sa vie privée et la vie privée en général vis-à-vis des technologies de sécurité

en général semblent même plus marquées que les craintes relatives à sa propre vie privée. En effet, au début de la journée, 75 % ont approuvé en Suisse l'affirmation selon laquelle les technologies de sécurité menacent de porter atteinte à la vie privée en général, soit une bonne dizaine de pour cent de plus que pour l'affirmation portant sur les craintes de voir sa vie privée personnelle menacée: 42 % se sont dits tout à fait d'accord, 33 % simplement d'accord. A ce sujet aussi, les résultats de la Suisse sont plus hauts que la moyenne de tous les pays, égale à 68 % – cependant, le phénomène selon lequel l'inquiétude pour la vie privée en général est plus prononcée que pour la vie privée personnelle est constaté dans tous les pays sauf l'Espagne. La conclusion s'impose que les conséquences de la surveillance sont perçues plutôt comme un danger abstrait, qui ne peut pas être mis sans autre en relation directe avec la vie quotidienne personnelle.

Même lorsque la conséquence des techniques de surveillance et la façon dont elles ont indûment accès à des informations d'ordre personnel sont décrites plus en détail, les craintes en Suisse restent moins marquées que dans la moyenne générale des pays participants. Les trois affirmations évoquant la crainte que des informations personnelles trop nombreuses ou inexactes soient collectées, sans le consentement de la personne concernée, obtiennent des valeurs élevées, soit un peu plus de 70 et 66 % («trop d'informations» sont collectées ou les informations peuvent être «inexactes»), voire 95 % («sans mon consentement») ; en moyenne dans tous les pays, la réponse à ces trois affirmations est positive dans 70 et 63 % des cas («trop d'informations» ou parfois «inexactes») et, s'agissant de la collecte de données sans le consentement de la personne, dans 90 % des cas.

Enfin, les participantes et les participants de Suisse considèrent un problème sous un jour un peu plus optimiste que la moyenne générale des pays : ici, ils sont au total 66 % à craindre que les informations collectées puissent être utilisées contre eux, contre presque 70 % en moyenne. Si on analyse plus en détail les catégories de réponses, les résultats se démarquent encore plus : en Suisse, 27 % sont tout à fait d›accord avec l'affirmation, contre 36 % en moyenne dans tous les pays participants.

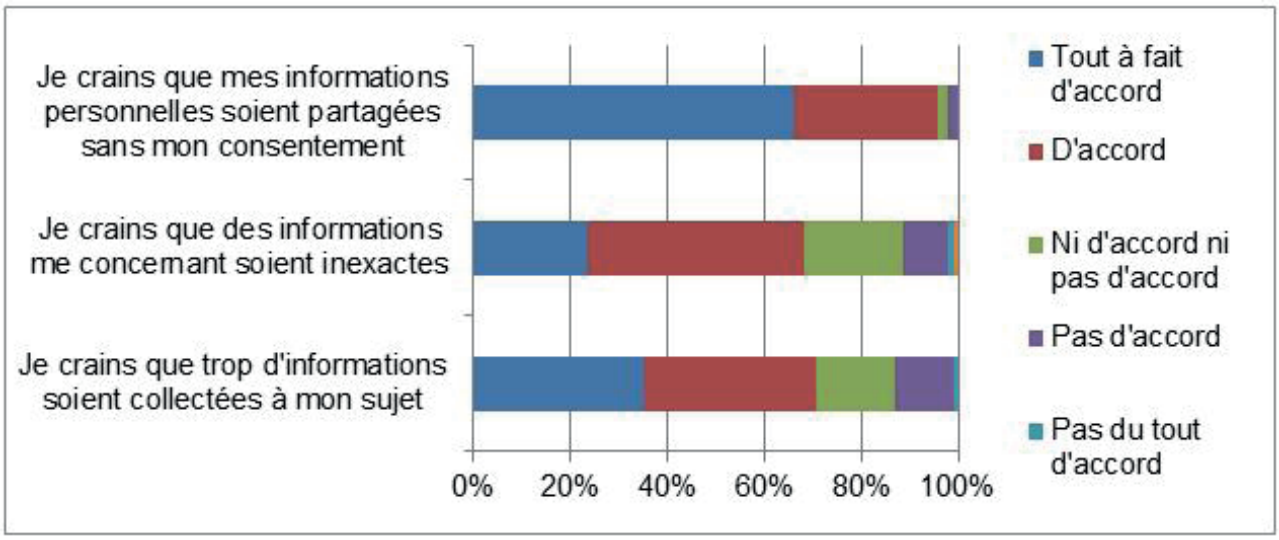

Figure 13: Inquiétudes entre la vie privée et les technologies de sécurité basées sur la surveillance en Suisse

C'est un indice qui plaide en faveur de l'hypothèse selon laquelle la collecte indue d'informations et ses conséquences sont souvent perçues comme étant légèrement moins graves en Suisse que dans beaucoup d'autres pays.

4.3. La jeunesse aussi attache beaucoup d'importance à la sphère privée

La protection de la sphère privée est une préoccupation aussi bien pour les jeunes que pour les moins jeunes ; dans la classe d'âge des 18 à 29 ans, au total 84 % se soucient de la vie privée en général et 70 % de leur propre vie privée.
Les plus jeunes donnent donc aussi un peu moins

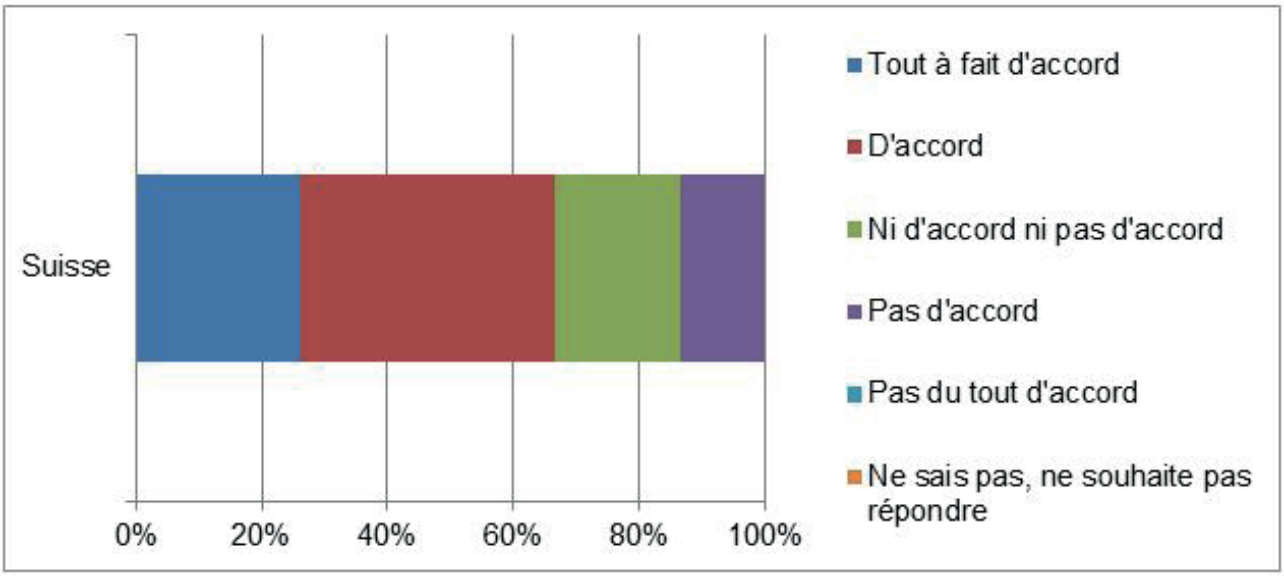

Figure 14: : «Je crains que mes informations personnelles soient utilisées sans mon contre moi.»

	N= 245	Tout à fait d'accord	D'accord	Ni d'accord ni pas d'accord	Pas d'accord	Pas du tout d'accord	Total
		Pourcentage					
18-39 ans	*38*	53	26	13	5	3	100
40-59 ans	*129*	43	35	14	5	1	100
Plus de 60	*78*	37	32	18	10	2	100

Figure 15: «Je crains que le recours aux technologies de sécurité basées sur la surveillance porte atteinte à la vie privée en général.»

de poids aux dangers pour leur vie privée personnelle qu'à ceux pour la vie privée en général. Cependant, en raison du faible nombre de cas, les résultats seront donnés dans la suite de ce rapport en regroupant les classes d'âge 18-29 ans et 30-39 ans.

L'affirmation selon laquelle les technologies de sécurité menacent la vie privée de façon générale a été approuvée pleinement par 53 % et sans plus par 26 % des 18 à 39 ans. De même, les deux catégories d'âge supérieures (40-59) souscrivent globalement en majorité à cette affirmation, mais la réponse «d'accord» atteint des scores plus élevés que «tout à fait d'accord».

En ce qui concerne les voix négatives, il n'est pas permis de conclure que la jeunesse accorde moins d'attention à la sphère privée. Certes, au total 8 % du groupe des 18 à 39 ans ont nié que les technologies de sécurité portent atteinte à la vie privée en général, dont 3 % de façon catégorique («pas du tout d'accord»).

En comparaison, seulement 6 % rejettent cette affirmation dans la classe des 40 à 59 ans (dont 1 % tout à fait). Mais dans la classe des plus de 60 ans, les soucis pour la sphère privée sont en revanche de nouveau moins prononcés – au total 13 % ont rejeté l'affirmation (2 % tout à fait, 10 % sans plus).

Ces résultats quantitatifs ne permettent en tout cas pas d'étayer l'hypothèse selon laquelle plus les gens sont jeunes, moins ils se soucie de la vie privée. Les résultats par âge confirment en outre que la préoccupation au sujet de la vie privée en général est plus prononcée que pour sa propre vie privée.

	N= 247	Tout à fait d'accord	D'accord	Ni d'accord ni pas d'accord	Pas d'accord	Pas du tout d'accord	Total
		Pourcentage					
18-39 ans	*38*	40	26	16	13	5	100
40-59 ans	*130*	29	40	20	11	0	100
Plus de 60	*79*	26	31	24	15	2	100

Figure 16: «Je crains que le recours aux technologies de sécurité basées sur la surveillance porte atteinte à ma vie privée.» selon l'âge (question posée au début de la manifestation)

4.4. La sphère privée dans les régions linguistiques de Suisse

Les gens craignent d'autant plus l'érosion de la sphère privée qu'ils évaluent plus positivement le niveau de leur propre sécurité et qu'ils rejettent plus fortement le recours général à des technologies de sécurité. Tel est du moins la conclusion que suggèrent les résultats quantitatifs classés par régions linguistiques.

A Zurich, où les gens se sentent le plus sûrs et où le recours général aux technologies de sécurité se heurte en même temps à la plus forte résistance, au total 80 % ont approuvé l'affirmation selon laquelle l'utilisation de ces technologie porte atteinte à la vie privée en général (48 % se sont déclarés tout à fait d'accord, 32 % d'accord). En ce qui concerne la vie privée personnelle, 72 % éprouvent des inquiétudes (35 % étaient tout à fait d'accord avec l'affirmation correspondante, 37 % d'accord).

Grandson se situe dans la moyenne suisse : au total, 77 % s'attendent à des atteintes à la vie privée en général (49 % tout à fait, 28 % sans plus). Ici aussi, les chiffres sont un peu inférieurs quand il s'agit du danger pour le

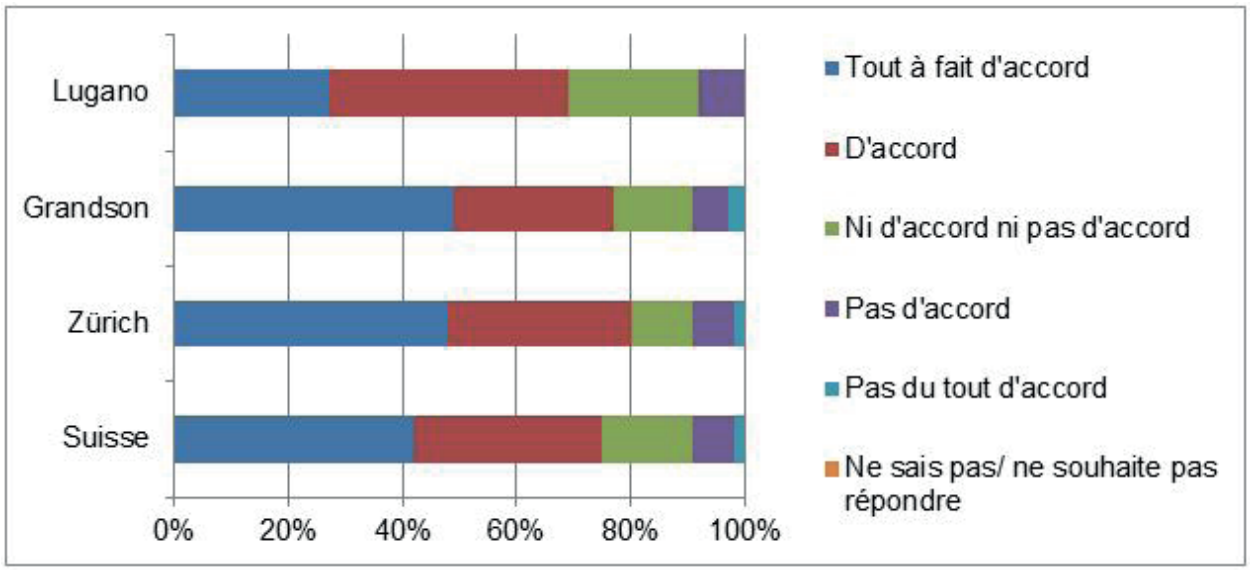

Figure 17: «Je crains que le recours aux technologies de sécurité basées sur la surveillance porte atteinte à la vie privée en général.»

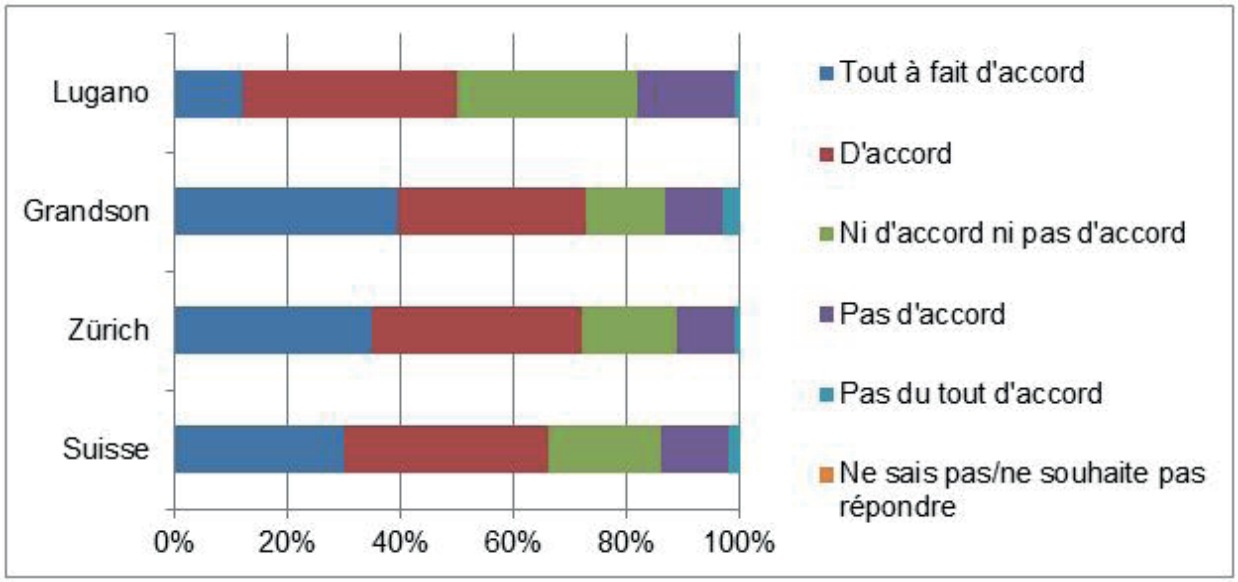

Figure 18: «Je crains que le recours aux technologies de sécurité basées sur la surveillance porte atteinte à ma vie privée.»

domaine privé intime : au total 72 % approuvent l'affirmation correspondante (39 % sont tout à fait d'accord avec elle, 33 % d'accord).

Au Tessin que les craintes d'une telle atteinte sont les plus faibles : au total, 69 % ont estimé que la vie privée en général est menacée (27 % étaient tout à fait d'accord avec l'affirmation, 4 % d'accord) et 50 % que tel est le cas de la vie privée personnelle (12 % étaient tout à fait et 38 % simplement de cet avis).
En ce qui concerne l'estimation de la menace sur sa propre vie privée, les différences à l'intérieur de la Suisse sont statistiquement significatives, alors que celles touchant aux menaces pour la vie privée en général n'atteignent pas le seuil de signification.

Ces constats suggèrent que le sentiment d'insécurité personnelle contribue à ce que la population 1 % accepte mieux les technologies de sécurité ou soit moins hostile à leur égard et consente plus facilement à des atteintes à la sphère intime. Il est possible que les chiffres reflètent aussi une certaine résignation ; Au Tessin notamment, l'impression prédomine que le privé est devenu déjà à tel point public qu'il n'y a plus grand chose à perdre : «Je sais que nous sommes surveillés, et parfois ça me fait peur – mais aujourd'hui, c'est comme ça».

5. Le Deep packet inspection (DPI) : des sérieuses réserves

Comme déjà relevé, le DPI désigne une technique de réseau qui permet d'examiner l'en-tête («Header») d'un paquet de données en fonction de certaines caractéristiques tels que spams, virus informatiques, violations de protocoles et autres contenus problématiques. Les données obtenues par SurPRISE montrent que cet instrument de surveillance des communications électroniques suscite de grandes réserves. Il convient cependant d'ajouter qu'il n'existe en Suisse aucune base légale qui permette de recourir au DPI pour sauvegarder la sécurité de l'Etat. En d'autres termes, il n'est pas permis aux autorités de ce pays de se servir de cet instrument. Cette question a ainsi été expliquée oralement par le modérateur et a été votée selon les conditions applicables en Suisse. Au total, pas loin de la moitié (47 %) des participantes et participants suisses accepteraient le DPI comme mesure destinée à renforcer la sécurité nationale, tandis que 34 % y seraient opposés. Notre pays est ainsi à peu près à égalité avec la moyenne des autres pays participants (45 % de voix pour contre 34 % de votes contre). Au sein du pays, les réponses à ce sujet correspondent aussi au sentiment de sécurité personnelle. Le DPI suscite tendanciellement le plus d'approbations (58 %) au Tessin, où les participantes et participants se sentent le moins sûrs. Grandson suit avec 43 % de votes favorables. C'est à Zurich (40 % de voix pour) que se sont exprimées les plus grandes réserves. Et comme pour le sentiment de sécurité personnelle, les différences entre les régions linguistiques au sujet de l'approbation du DPI sont significatives.

En regardant les utilités du DPI en tant que sécurité nationale, il se produit en Suisse un modèle d'opinion déjà familier. Au Tessin l'utilisation du DPI comme mesure pour la sécurité nationale a obtenu le score le plus élevé avec 40 % de vote, et le taux le plus bas à Zurich avec environ 30 %. Ces différences sont statistiquement significatives. À Grandson, une différence intéressante est observée: plus de 40 % des participants soutiennent le DPI comme étant un instrument efficace pour protéger la sécurité nationale. Cependant, un peu moins de 27 % a également estimé que son utilisation est appropriée (contre 30 % à Zurich et 45 % dans le Tessin. A Grandson l'écart entre l'efficacité et la pertinence est la plus évidente.

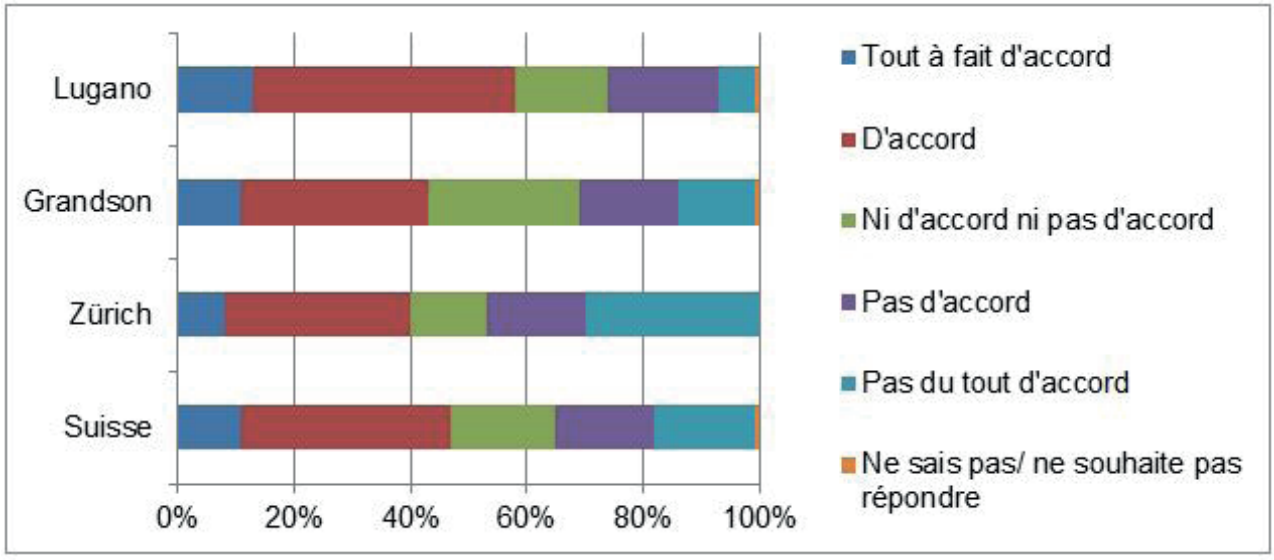

Figure 19: «Dans l'ensemble, je soutiens le DPI comme mesure pour la sécurité nationale.»

Ou, en d'autres termes, c'est l'efficacité de la méthode qui émet des réserves quant à cette technologie

5.1. Le DPI divise l'opinion et porte atteinte à la sphère privée

Le DPI divise l'opinion et porte atteinte à la sphère privée Le recours au DPI vise différents objectifs. Il sert par exemple à détecter des programmes nocifs et protège donc aussi les ordinateurs des utilisatrices et utilisateurs. Mais cette technique peut être appliquée également par des services de l'Etat à des fins policières ou de renseignement, voire pour surveiller ou opprimer les citoyens d'un Etat répressif. Les réponses des personnes participant à SurPRISE montrent que celles-ci ne tiennent pas en haute estime l'utilisation de cette technique pour leur sécurité personnelle et qu'elles lui font peu confiance. Un tiers environ étaient d'avis qu'un recours au DPI protègerait efficacement et de façon adéquate les intérêts de la Suisse en matière de sécurité. Les proportions de celles et ceux qui ont rejeté cette vision des choses ou qui ne se sont pas déterminés étaient à peu près les mêmes. Le DPI a été jugée de façon franchement plus négative dans l'optique du sentiment de sécurité personnelle. Seulement 6 % des participantes et participants ont été d'avis qu'elles se sentiraient plus sûres quand elles naviguent sur le web si le DPI était utilisé, tandis que 73 % ont rejeté cette appréciation. L'opinion est mitigée aussi dans les autres pays participants, même si à l'exception de l'Autriche et de la Norvège, ils ont eu tendance à évaluer le DPI de façon un peu plus positive que la Suisse pour la sécurité individuelle sur le web.

Les données quantitatives indiquent que le scepticisme à l'égard du DPI a toutes sortes de motifs. La vision des choses qui se dégage des forums de discussion suisses ne diffère pas fondamentalement de celle dans d'autres pays. Le fait que des comportements d'utilisateurs puissent donner lieu à malentendu, des informations personnelles parvenir à des tiers, voire des droits humains fondamentaux être violés, a suscité, chez de nombreux participants et participantes à Zurich, Grandson et Lugano, des inquiétudes qui se sont exprimées aussi au niveau qualitatif lors des discussions.

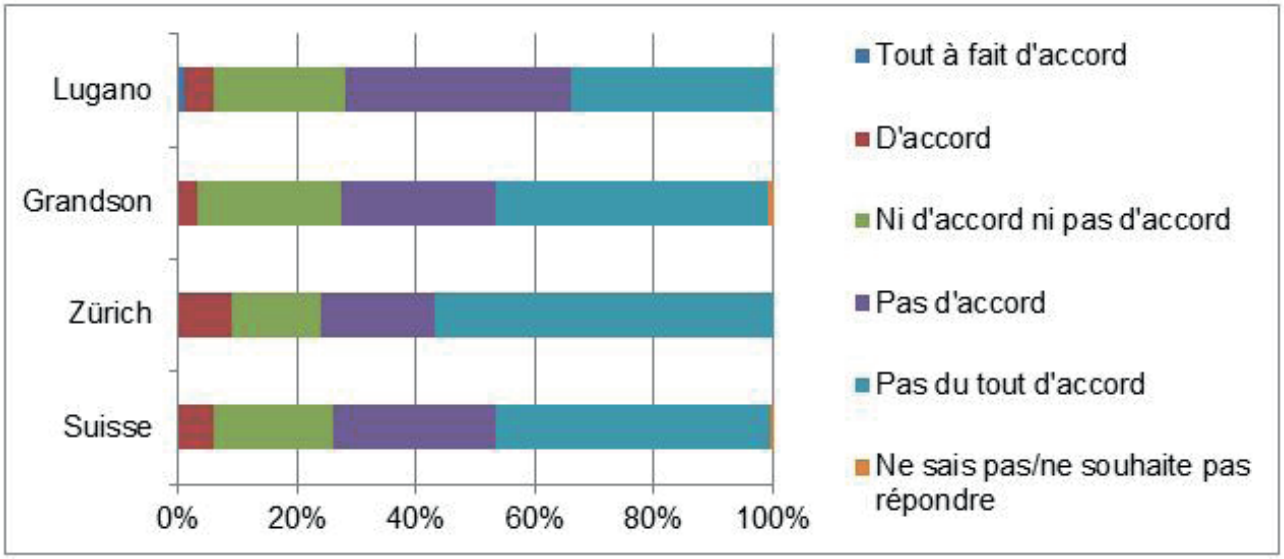

Figure 20: «Quand je suis en ligne, je me sens d'avantage en sécurité grâce au DPI.»

5.2. «Qui contrôle – et qui contrôle les contrôleurs ?»

Le manque de transparence a donné beaucoup à discuter, et ceci dans les trois régions linguistiques. La question de savoir qui exactement recourt au DPI et dans quels buts inquiète beaucoup de citoyennes et citoyens. «On ne sait pas qui contrôle le DPI : des sociétés privées ou des gouvernements, parfois des Etats incompétents pour la régulation», craint par exemple quelqu'un, tandis que d'autres font remarquer : «Il y a un manque de transparence. Qui contrôle quoi – et qui contrôle les contrôleurs» et «J'aimerais savoir qui contrôle les données et à quoi on prête attention. Cette perte de contrôle est gênante». Enfin, quelqu'un pense : «Il y a toujours le problème du contrôle des contrôleurs. Il faut des commissions – et de la transparence. Car nous ne savons pas qui contrôle quoi»

Les critères qui font que quelqu'un se trouve finalement dans le collimateur des autorités sont tout aussi opaques. «Qui décide qui sont les criminels potentiels ?». A cette question, quelqu'un répond : «C'est nous qui décidons qui sont les bons et les méchants ; c'est une question éthique et morale». La situation manque de clarté et pas seulement à propos des responsabilités lors du recours au DPI – les processus eux-mêmes sont opaques. «Qui définit les mots-clés (qui font l'objet d'une recherche)? Ce sont en partie des mots de tous les jours, par exemple «vacances». Si un mot-clé est général, nous sommes tous concernés quand nous communiquons sur le réseau.»

A part le fait qu'un bon nombre de participantes et participants ont plaidé lors des discussions pour davantage de transparence, de nombreuses cartes postales ont également abordé cette thématique, «davantage de transparence!», exige laconiquement quelqu'un de Zurich, tandis qu'une autre personne demande de façon plus détaillée et radicale : «Davantage de transparence sur le terrorisme technologique moderne». Le ton est semblable à Grandson : «Transparence, transparence, svp. Le public en général est tenu dans l'ignorance de ce qui est réellement fait de ces données personnelles». Au Tessin, une personne exige par exemple que ces nouvelles technologies soient utilisées de façon transparente et éthique.

Le mélange d'acteurs et d'intérêts de l'Etat et de l'économie privée hérisse quelques personnes ; et beaucoup sont indignés par une possible utilisation commerciale des données : «Il n'y a pas de transparence, les données aboutissent dans la publicité. Le défi consiste à faire la transparence et à réglementer sur une base éthique». D'autres s'expriment de façon similaire : «La séparation étatique et commerciale n'est pas évidente. L'éthique est très basse. Les Länder allemands achètent des données de banques – est-ce étatique ou commercial ? Cela est très dangereux.» Enfin, quelqu'un plaide pour que l'on n'autorise pas tous azimuts tous les systèmes de surveillance, surtout pas pour des raisons commerciales. En tout et pour tout, de nombreuses prises de position confirment que les autorités jouissent d'un haut degré de confiance et que presque personne ne craint qu'elles recourent à des moyens techniques au détriment des citoyennes et citoyens. Plus d'une fois, les participantes et participants ont relevé que les régimes totalitaires tendent à utiliser les puissantes possibilités techniques contre leur propre population. Par conséquent, les effets d'une technologie de surveillance pour les individus peuvent différer fortement suivant dans quelles mains elle tombe. Quelqu'un exprime l'essentiel comme suit : «Je suis conscient du fait que je suis sous surveillance. En Suisse, ce n'est peut-être pas si grave, mais en Corée du Nord je serais inquiet».

5.3. L'homme est plus que ses données

De l'avis des participantes et participants de toutes les régions linguistiques, le DPI a une forte incidence sur les droits de la personnalité. Le fait qu'à l'insu des gens, des données

parviennent entre des mains étrangères n'est qu'un des nombreux problèmes. Les données volées peuvent conduire à de fausses interprétations et entraîner de graves conséquences pour les personnes concernées.

Dans les trois régions linguistiques, des participantes et participants ont exprimé la crainte que des surveillances infondées puissent avoir lieu et qu'en raison de malentendus et de fausses interprétations, des innocents entrent dans la ligne de mire des contrôles étatiques. Une personne met en garde contre une transformation corrélative de la conception du droit : «Jusqu'à maintenant, la présomption d'innocence était de rigueur. Avec la surveillance, nous passons à un régime de suspicion générale. Quels critères appliquer ? C'est là une importante question fondamentale.»

Finalement, nombre de participantes et participants des différents forums de discussion craignent les changements sociaux qu'une technique comme le DPI menace de promouvoir. Ils ont exprimé à plusieurs reprises l'inquiétude que seuls des gens fortunés pourront se protéger contre le harcèlement électronique ou engager des avocats compétents pour se défendre contre des accusations. «Si quelqu'un est traqué qui n'a pas de moyens, il ne peut pas se défendre», a constaté quelqu'un. De même, un faible niveau de scolarité accroît, du point de vue de quelques participantes et participants, le danger que des personnes ne sachent pas comment parvenir à des informations sur la surveillance électronique et sur de possibles contremesures. Le DPI est également perçu comme un instrument qui, à différents égards, ouvre la voie à la société à plusieurs vitesses, et qui peut aussi déboucher sur un classement «selon le schéma X»: «Google adapte les réponses à mes requêtes en fonction de mes recherches antérieures. Cela signifie que tout reste enregistré quelque part et que je suis mis en quelque sorte dans un tiroir, qu'on établit mon profil et qu'après un certain temps on préétablit pratiquement quels sont mes intérêts, mes préférences etc.»

5.4. Les avantages ne compensent pas les inconvénients

Lors de tous les forums de discussion, les participantes et participants ont abordé aussi les avantages que le DPI leur semblait procurer. La défense contre les spams et les virus informatiques a été plusieurs fois nommée lors de ces forums, de même que la lutte contre la pédophilie. Comme exposé plus haut, les résultats de l'enquête quantitative permettent cependant de conclure que nombre de ces avantages du DPI ne pèsent pas lourd dans l'optique de la sécurité informatique individuelle.

Le contrôle à grande échelle des données comme moyen permettant de mettre un terme aux activités terroristes a rencontré à plusieurs reprises des échos positifs, mais a paru toutefois discutable à nombre de personnes. Plusieurs d'entre elles ont déploré l'absence de données permettant de mesurer effectivement combien d'attentats contre la sécurité nationale ont été vraiment empêchés grâce au DPI; elles ont critiqué le fait que les succès et échecs de ces surveillances n'ont pas fait l'objet d'évaluations. D'autre part, les malfaiteurs ont en règle générale de très bonnes connaissances techniques et sont capables de prendre des mesures pour ne pas être découverts prématurément : «Les criminels sont plus malins que nous, ils ne se consultent pas par courriel s'ils préparent l'enlèvement de Tettamanti». En tout et pour tout, le DPI est très coûteux par rapport aux succès il permet d'obtenir : «Le nombre de malfaiteurs capturés grâce au DPI est extrêmement bas et ne justifie pas cette surveillance à très large échelle», souligne quelqu'un.

6. Géolocalisation des smartphones : Des avantages pas contestés

A part le DPI, le débat mené dans la cadre de SurPRISE a aussi porté sur la géolocalisation via les téléphones portables. En Suisse, la localisation d'un téléphone n'est autorisée que dans le contexte d'une enquête juridique ou policière – par exemple s'il s'agit d'élucider un crime. La vidéo qui a servi d'introduction aux discussions a abordé aussi bien la localisation qui peut avoir lieu chaque fois qu'un téléphone portable communique avec les antennes relais que celle recourant au GPS, possible seulement pour les smartphones. Alors que la localisation dans le réseau d'antennes relais est fondée sur le mode de fonctionnement des téléphones portables, celle par le GPS se base en premier lieu sur différentes apps.

Lors des discussions, les participantes et participants n'ont souvent pas mentionné exactement à quel type de géolocalisation leur avis se référait. En dépit de ce léger flou terminologique, il est néanmoins clairement ressorti – exactement comme pour le DPI – que la géolocalisation ne jouit pas d'une approbation sans réserve en Suisse. En comparaison de la moyenne de 58 % pour l'ensemble des pays participant à SurPRISE, l'approbation de la géolocalisation comme moyen de protection de la sécurité nationale a atteint en Suisse un score un peu plus bas de 55 %. La géolocalisation s'est donc assuré néanmoins une petite majorité des voix. Reste qu'un bon quart des participantes et participants ont rejeté l'affirmation préconisant l'approbation de cette technique comme instrument de protection de la sécurité nationale. Comparé aux taux d'approbation de 47 % et de rejet de 34 % que le DPI a obtenus dans notre pays, la géolocalisation s'assure des cercles un peu plus larges de partisans. Sur cette question, l'opinion en Suisse est en phase avec celle dans les autres pays participants, qui ont également souscrit en majorité à la géolocalisation des téléphones portables – à l'exception toutefois de l'Allemagne : dans ce pays, les réserves sont si grandes qu'une minorité d'à peine un tiers seulement s'est déclarée favorable au recours à la géolocalisation comme mesure de sécurité pour la nation.

L'acceptation relativement large de la géolocalisation pourrait dépendre du fait que ses avantages sont directement perçus dans la vie de tous les

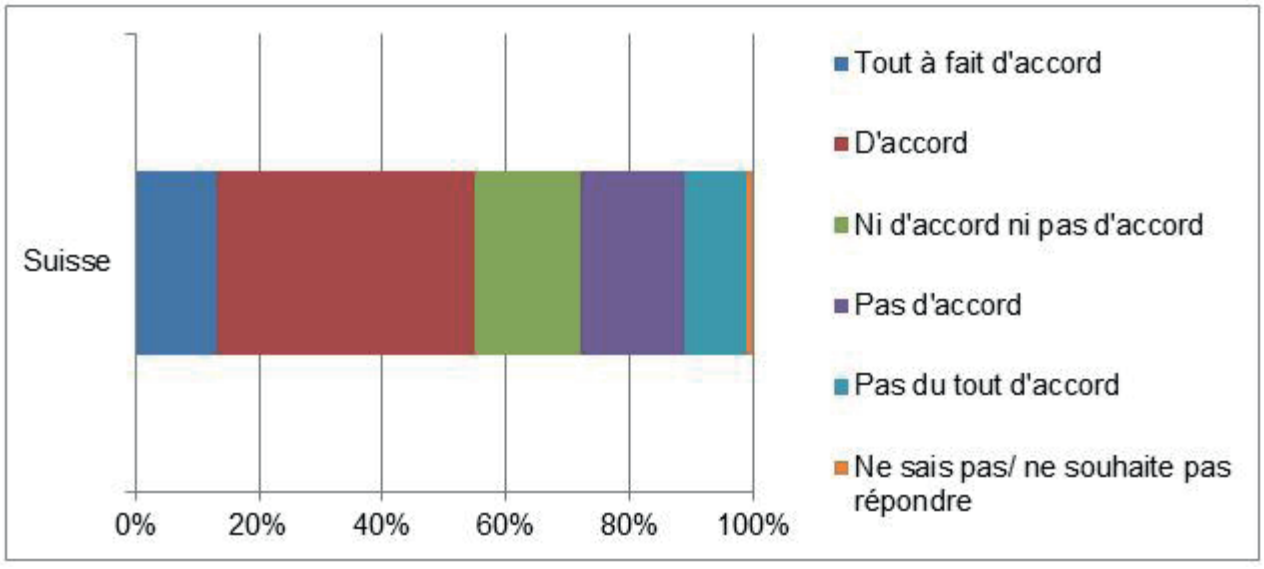

Figure 21: «Quand je suis en ligne, je me sens d'avantage en sécurité grâce au DPI.»

jours : «C'est très souvent pratique.
Si tu cherches le bus, il te montre la station la plus proche. De temps en temps, je me sers de ça» », a dit quelqu'un. Le fait que grâce aux fonctions de localisation de leur téléphone portable des personnes qui ont disparu sont repérées ou d'autres qui se sont perdues sont capables de s'orienter a été mentionné dans tous les forums de discussion comme un solide avantage. Le tracking est reconnu comme pratique aussi pour retrouver un téléphone portable perdu, ou encore pour suivre des transports à risque. D'autres applications utiles citées sont les alertes routières aidant les conducteurs à choisir leur itinéraire et les mesures du trafic pouvant être mises à profit pour la planification urbaine et routière.

6.1. Des coulisses plus transparentes

La technique de géolocalisation ne présente pas seulement des avantages tangibles, mais possède aussi un «visage institutionnel» : ses utilisatrices et utilisateurs savent qui est leur fournisseur de services, ce qui leur permet de se faire une idée de qui conserve leurs données et dans quel but. Ou en d'autres termes : les utilisatrices et utilisateurs ont une idée de ce qui se passe derrière les coulisses et qui est responsable pour cela. La géolocalisation par le biais des antennes, en tous cas, semble être un inconvénient secondaire qui est accepté. «L'opérateur de téléphonie mobile à toutes ces données. La question est de savoir si je peux simplement venir et lui demander où se trouve ton téléphone portable. C'est ça la question.», ont estimé en substance des personnes dans toutes les régions du pays. D'aucuns ont vu aussi la raison administrative de cette récolte de données : «Ils doivent conserver cela aussi pour qu'on puisse mettre en doute ou justifier une facture. Ça ne me paraît pas si bête ces six mois» a complété une personne.

Plusieurs participantes et participants ont été unanimes à penser que si l'on compare explicitement le DPI et la géolocalisation, cette seconde technique de localisation se présente comme plus transparente et offre de plus grandes possibilités d'exercer une influence. «Dans le cas du téléphone portable, c'est un peu plus facile d'avoir une influence. On peut éteindre des choses. On a une plus grande marge d'autodétermination qu'avec le DPI», a avancé quelqu'un , «Il est plus facile de réglementer à ce sujet, du moins en Suisse, que pour le DPI», a complété une autre personne à Zurich. Plusieurs participantes et participants ont relevé la possibilité simple de déjouer d'éventuels espions en remettant son propre téléphone portable à une autre personne. «La géolocalisation révèle où vous êtes, mais pas ce que vous faites», a résumé quelqu'un.

6.2. Faire face aux risques de la géolocalisation

En dépit de l'utilité manifeste de la géolocalisation des téléphones portables, nombre de personnes ont fait état d'inconvénients de cette technique. Il leur a semblé particulièrement choquant que des privés puissent avoir accès aux données. «Je ne souhaite pas recevoir de réclame pour du chocolat sur mon téléphone portable», a relevé quelqu'un. Des déclarations similaires ont été faites dans tous les forums de discussion. Pourtant, les services de l'Etat ne semblent pas non plus au-dessus de tout soupçon. «Le danger existe que des adversaires politiques soient surveillés, par exemple lors de manifestations.», ont craint divers participantes et participants dans toutes les régions linguistiques.

La pression sociale et les risques d'exclusion sont aussi un aspect qui préoccupe les participantes et participants en relation avec la géolocalisation. De façon tout à fait générale, la dépendance au téléphone portable en a fait réfléchir plus d'un, et en ce qui concerne la technique de géolocali sation, plusieurs personnes ont craint que la lecture des cartes topographiques se perde en tant que technique culturelle. «La localisation présente l'inconvénient que les jeunes n'apprennent plus à

se repérer sans elle», a relevé quelqu'un. Et une autre personne de compléter qu'elle craignait de se rendre suspecte quand elle éteignait son téléphone portable pour ne pas être localisée.
Le manque de transparence a donné lieu à critique aussi dans le cas de la géolocalisation – encore que les griefs sont dirigés dans ce cas en premier lieu contre les applications («apps») qui se servent des données de localisation à l'insu des utilisatrices et utilisateurs. Les participants et participantes ont mis en cause les conditions d'utilisation souvent volumineuses et confuses, que presque personne ne lit si l'on veut installer une application rapidement. En outre, dans tous les forums de discussion, des personnes ont réclamé avec insistance que la fonction de géolocalisation soit désactivée par défaut sur les téléphones portables ; elle ne devrait être activée que si l'utilisateur ou l'utilisatrice donne expressément son consentement.

6.3. La main haute sur la technique

L'enquête quantitative n'a pas seulement exploré l'opinion des citoyennes et citoyens quant aux instruments de la surveillance, mais a cherché aussi à se faire une image des acteurs qui se servent de ces techniques.
Dans le cas de la Suisse, les résultats attestent que les participantes et participants font assez largement confiance aux autorités dans notre pays. Des organes de sécurité qui viendraient à recourir au DPI jouissent chez nous de plus de confiance qu'en moyenne dans les pays participants. On a bon espoir qu'à part les intérêts de la sécurité nationale, ces organes respecteraient le cas échéant aussi ceux des citoyennes et citoyens.

Environ 25 % des participantes et des participants suisses considèrent que les autorités ne sont pas dignes de confiance – soit une valeur sensiblement inférieure à la moyenne générale des pays participants, qui est de 35 %. Toutefois, il faut tenir compte du fait que près d'un tiers (28 %) des personnes interrogées s'inscrivent dans la catégorie des indécis «ni d'accord ni pas d'accord».
Ce résultat ne peut pas être interprété sans autre : il pourrait signifier que les personnes interrogées ont du mal à évaluer dans quelle mesure les institutions compétentes sont dignes de confiance.

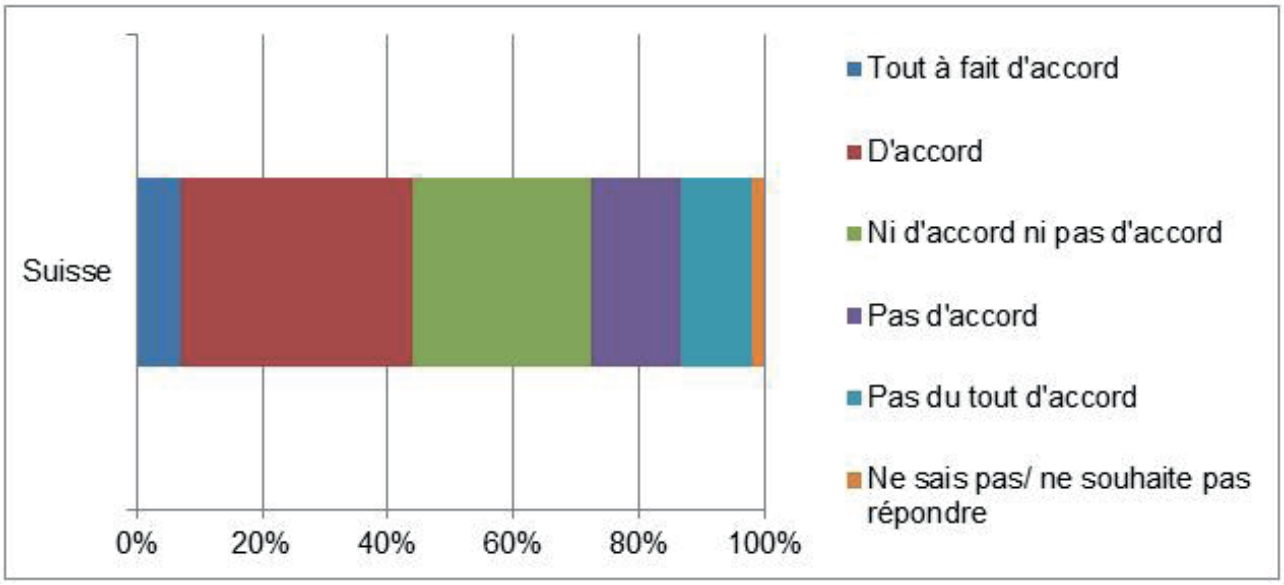

Figure 22: «Les agences de sécurité qui utilisent le DPI sont dignes de confiance.»

Il serait aussi possible que le caractère hypothétique de la question suscite des difficultés ; en tous cas, plusieurs personnes dans le public ont demandé de quelles autorités il s'agissait, parce qu'en Suisse, les instances publiques n'ont pas le droit de recourir au DPI.

En tous cas, les participantes et les participants de Suisse sont très confiants dans le fait que les autorités compétentes ne perdraient pas de vue les intérêts des citoyennes et des citoyens si elles utilisaient le DPI pour défendre la sécurité nationale : 40 % des réponses vont dans ce sens, alors que la moyenne générale des pays est de 33 %. Les participantes et participants suisses sont plus sceptiques que celles et ceux des pays voisins uniquement à propos de la compétence des autorités.

Dans notre pays, 25 % sont d'avis que si le DPI était utilisé, les institutions concernées sauraient ce qu'elles font – contre 27 % en moyenne de tous les pays participants.

Pour le recours à la géolocalisation par le biais du smartphone, les autorités suisses obtiennent un score encore plus favorable que pour celui – hypothétique – du DPI. Dans ce cas, il y a même une bonne majorité de 57 % des participantes et participants pour défendre le point de vue que la confiance se justifie – contre en moyenne 46 %.

Pour toutes les autres qualités, telles que la compétence, l'attention à l'égard des intérêts des citoyennes et des citoyens et le renoncement à l'abus de pouvoir, les Suissesses et les Suisses ont une plus haute idée de «leurs» autorités que cela est le cas en moyenne de tous les pays participants. Lorsqu'il s'agit du recours à la géolocalisation, l'image des autorités de sécurité est donc meilleure qu'au sujet du DPI.

7. Recommandations-Des doutes quant à la possibilité d'imposer des solutions

En conclusion des journées, les participantes et participants ont discuté de solutions possibles pour atténuer les inconvénients des technologies de surveillance et diminuer le malaise que ces dernières suscitent. En complément, ils ont consigné la quintessence de la discussion qui avait eu lieu à leur table. La liste des recommandations ainsi obtenues est jointe au présent rapport. Ces débats de clôture sur des mesures possibles ont été souvent marqués par des doutes quant à la possibilité d'imposer les propositions faites, voire par un sentiment de résignation.

7.1. Conventions et lois

Lors de tous les forums de discussion, les participantes et participants ont demandé expressément que des garde-fous efficaces soient inscrits dans la législation. Mais en même temps, la possibilité de réaliser cette exigence a été mise en doute à toutes les tables de discussion : en effet, l'expérience montre d'une part que la législation est constamment en retard sur la technique ; d'autre part, légiférer au niveau national a peu d'influence pour infléchir le flux de données mondial dans la bonne direction. «Je n'ai pas foi en la loi, parce qu'une loi est toujours en retard sur la technologie.

C'est pourquoi il est si difficile de savoir comment poser des limites à cet égard, des limites par la législation. Et de savoir à quels instruments recourir pour sanctionner les infractions. On pourrait faire une comparaison avec les droits de l'homme, qui sont aussi violés sans arrêt, sans que rien ne se passe». estime par exemple une personne à Zurich. Et quelqu'un à Grandson est convaincu que « la technique va beaucoup plus vite que les politiciens, ça ne sert donc à rien de faire des lois sur ces technologies qui seront démodées lorsque la loi sera édictée». Des déclarations similaires ont aussi été faites à Lugano. Les différentes conceptions du droit et convictions morales dans le monde alimentent également des doutes quant à l'applicabilité des lois – sans même parler d'intérêts divergents. «Il faudrait que l'intégralité des pays mette en place une législation commune. C'est quasiment impossible», résume quelqu'un. Et une personne à Zurich de penser : «Il faut une instance supérieure qui impose cela (une réglementation, réd.). Et quelle instance serait en mesure d'imposer à chaque pays de céder un peu de sa souveraineté?» Le ton est au pessimisme aussi à Lugano : «Même si nous avons une réglementation, elle ne s'applique pas en Amérique». Une personne à Grandson a fait remarquer que des lois plus sévères pourraient désavantager un pays : «Si l'Europe est réticente, les USA vont en profiter pour instaurer leur pouvoir économique. Je ne vois pas comment lutter, si nos lois sont plus sévères, les USA en profiteront. »

Dans les trois régions linguistiques, différentes personnes se prononcent dans ce contexte en faveur de directives éthiques générales qui préconiseraient le respect de l'humain et de sa vie privée et garderaient leur validité indépendamment des nouveaux développements technologiques.

Néanmoins, un léger espoir subsiste pour que les technologies de surveillance ne se soustrairont pas toutes au même degré à une réglementation légale. Pour différents participants et participantes à SurPRISE, un avantage de la géolocalisation au moyen du smartphone réside dans le fait qu'elle peut donner lieu à des dispositions nationales :«Ici au moins, réglementer seulement au niveau suisse est plus facilement possible que pour le DPI», a-t-on entendu à Zurich, et en substance aussi à Grandson

7.2. Contrôle et droit d'auteur

Une grande préoccupation des citoyennes et citoyens participant à SurPRISE est aussi de garder le contrôle sur leurs données, ce qu'une personne à Zurich a résumé en ces mots : «J'aimerais savoir qui contrôle les données et à quoi on prête

attention. Cette perte de contrôle est gênante». Des déclarations allant dans le même sens ont été entendues également à Grandson et à Lugano. A cet égard, il a été fait appel à plusieurs reprises à une plus forte protection des données. «Si des milliards sont mis dans la surveillance, il faudrait également investir des milliards dans la protection des données.», a constaté quelqu'un à Grandson. A Zurich, un des groupes de discussion a défendu l'idée d'un préposé mondial à la protection des données.

Des mesures de précaution techniques pourraient contribuer à répondre au scepticisme à l'égard de la surveillance. A Zurich, une voix s'est élevée pour dire : «Il devrait être possible aussi de pouvoir effacer les données. Il existe des logiciels où un message expire après peu de temps. Il devrait donc être possible techniquement que des choses soient effacées». En Suisse romande et italienne aussi, on a réclamé une «gomme numérique» qui fasse en sorte que des données ne restent pas indéfiniment en mémoire. «Pour cette histoire de confiance, il serait essentiel que l'expéditeur ait un droit d'auteur. Que tu puisses décider si quelque chose doit être effacé ou modifié. Ce serait vraiment essentiel.», a estimé une autre personne . Une personne, à Grandson, a quant à elle fait état de conséquences négatives possibles en relation avec l'effacement d'informations : «Effacer peut être problématique, parce que les victimes d'abus se manifestent souvent très tard».

7.3. Transparence et évaluation

Le désir de contrôle est étroitement lié à l'aspiration à plus de transparence. «Si tu connais la source, tu peux suivre ce qui se passe. C'est à cause du manque de transparence qu'on n'arrive pas à comprendre ce qui nous arrive.» Ici et là, c'est même une transparence globale qui a été exigée, au sens d'une renonciation au secret et à la sphère privée – une personne était convaincue que si tout est ouvert, il ne peut y avoir d'agissements malfaisants «Le problème est l'anonymat. Nous discutons sur la protection des données, parce qu'il n'y a pas de transparence au sujet des expéditeurs. L'anonymat est le problème. Une approche de solution serait que l'auteur doive être connu. Quiconque se connecte devrait se faire connaître. La technologie permettrait de savoir qui a commis quel abus. La loi est inefficace pour faire face à ce problème».

Différents participants et participantes de tous les groupes de discussion ont relevé que des données fiables ne font pas défaut seulement à propos du recours au DPI et à la technique de localisation, mais qu'il n'y a pas non plus de contrôle des résultats : «Les services secrets disent : si rien ne se passe, c'est parce que nous avons bien surveillé. Et si quelque chose se passe, ils disent qu'il faut surveiller d'avantage.», a dit sans détour une personne à Zurich «Il faudrait avoir des statistiques pour savoir ce qui a été empêché par la surveillance», a exigé quelqu'un d'autre. L'éventualité que les autorités donnent suite à cette demande a rencontré des doutes. Une personne a décrit la situation comme suit : «Le problème tient aux intérêts en jeu. Beaucoup ont intérêt à rester anonymes. Aussi l'Etat, si des services secrets font quelque chose. C'est pourquoi l'idée de la transparence totale n'est pas applicable. Ce qui se cache là derrière est en fin de compte une affaire de pouvoir. Si tu as des informations sur quelqu'un, tu as du pouvoir. Et c'est voulu. On ne veut pas que tous soient à armes égales»

7.4. Comportement individuel et pouvoir des consommateurs

Du fait qu'ils attendent peu de chose de garde-fous régulateurs, bon nombre de participantes et participants misent sur la responsabilité individuelle. «On peut imaginer éventuellement d'atténuer les conséquences au niveau individuel. On peut faire cela en informant, pour que les gens sachent ce qui est lu et enregistré», ont suggéré différentes personnes à Grandson et à Zurich, tandis que quelqu'un à Lugano a défendu

l'idée de mises en garde pour les applications indiscrètes sur le web ou sur les smartphones, un peu comme les avertissements dissuasifs sur les paquets de cigarettes : «L'utilisateur devrait toujours connaître les risques. On pourrait le prévenir : votre courriel pourrait être lu / vos données seront peut-être enregistrées.»

Dans ce contexte, plusieurs participantes et participants ont relevé que la clientèle a un pouvoir sur le marché. Quelqu'un a rappelé que même Facebook a amélioré sa protection des données lorsque toujours plus de jeunes se sont distancés de ce réseau social. «En tant qu'utilisateurs de smartphones, nous sommes une masse de consommateurs. On pourrait penser que nous avons de ce fait un certain pouvoir. Si nous nous mettons ensemble et savons nous entendre. On peut aussi NE PAS choisir certaines apps si on sait qu'elles transmettent nos données plus loin», a estimé une des personnes».

Tous n'ont pas partagé cet optimisme, comme en témoigne ce point de vue exprimé dans le même forum de discussion : «Ce sont toujours les mêmes géants qui sont derrière les apps intéressantes. En ce qui concerne la clientèle, je suis plutôt sceptique, car il est difficile de faire jouer la concurrence entre les fournisseurs.» Toutefois, tous ont été d'accord que les conditions générales et les conditions d'utilisation devraient être plus intelligibles et plus conviviales.

Plus d'une fois, il a aussi été fait mention de la possibilité de «maquiller» ses propres communications électroniques par un choix approprié du langage et de la terminologie. «Chacun doit commencer par lui-même et faire attention. Et chacun doit crypter, coder son propre langage» a fait valoir quelqu'un. Une autre personne a fait état des moyens techniques d'autoprotection, tout en relativisant les chances de succès de cette approche : «Il faut crypter – mais les gens ne veulent pas, ça fait espionnage».

Cependant, des voix se sont exprimées pour dire que ce sont précisément les changements de comportement dus à la surveillance électronique qui comptent parmi les risques sociaux les plus importants : «C'est mon principal souci. Si tous pensent qu'ils doivent s'exprimer de façon très prudente, une énorme part de spontanéité et de confiance se perdra. Si nous nous abordons les uns les autres avec méfiance, nous devons nous demander ce qu'il adviendra de notre âme» a précisé quelqu'un.

Les résultats de l'enquête quantitative confirment que les technologies de surveillance ont certainement un impact sur le comportement humain. En Suisse, 44 % des participantes et participants à SurPRISE ont indiqué vouloir se comporter autrement que jusqu'ici à cause du DPI – contre 54 % qui ne peuvent pas s'imaginer cela. A cet égard, des différences significatives se manifestent entre les régions linguistiques. En Suisse alémanique, 57 % prennent en considération un changement de comportement lors de leurs activités en ligne (contre 36 % qui ne le font pas). Au Tessin, 45 % examinent de possibles mesures de prudence (contre 60 % qui continuent de se comporter comme jusqu'ici). En Suisse romande enfin, 38 % envisagent d'adapter leur comportement quand ils naviguent sur le web (contre 60 % qui gardent leurs habitudes).

Dans le cas du smartphone, la propension à modifier son comportement est nettement moindre. Seulement 25 % ont déclaré vouloir renoncer totalement au téléphone portable ou adapter leur comportement de manière à ne pas être localisés. Par contre, 69 % des participantes et participants n'ont pas l'intention de changer leur comportement. Ces chiffres sont comparables aux moyennes de tous les pays participant à SurPRISE. Toutefois, des différences significatives sont constatées à l'intérieur de la Suisse. Cette fois, ce sont les participantes et participants de la Suisse romande qui songent le plus à modifier

leur façon d'agir (31 %). Au Tessin, 25 % des personnes pensent adapter leur comportement, et en Suisse alémanique seulement 13 %.
Les discussions ont effectivement fourni des indices selon lesquels de subtils changements ont lieu dans le comportement des gens. Plusieurs personnes ont relevé que le besoin de contrôler ses propres données a pour effet d'assécher des canaux d'information établis. Par exemple, beaucoup de gens ne se font plus inscrire dans l'annuaire téléphonique officiel de Swisscom. «Il est effrayant de voir combien de personnes déménagent sans communiquer leurs données. Elles ne veulent pas de publicité, pas d'appels – on constate un changement dans la société. On sombre dans l'anonymat, on ne trouve plus les gens. Ils ont quatre ou cinq adresses de contact par courriel et plusieurs téléphones portables, mais on ne les trouve plus», a observé une des personnes. Et quelqu'un d'autre se dit «étonné par le décalage entre l'application des lois sur la protection des données (par exemple lorsqu'on recherche l'adresse de quelqu'un et qu'il est très difficile de l'obtenir) et toutes les données auxquelles nous avons accès librement sur Internet». Dans ce contexte, plusieurs participantes et

Deep Packet Inspection *(N=248)*		Géolocalisation des smartphones *(N=248)*	
Pourcentage			
Je n'irai pas sur Internet à cause du DPI	1	Je n'utiliserai pas un smartphone à cause de la géolocalisation des smartphones	3
J'éviterai d'aller sur Internet à cause du DPI	4	J'éviterai d'utiliser un smartphone à cause de la géolocalisation des smartphones	5
Je ne changerai pas de comportement en ligne à cause du DPI	40	Je changerai de comportement à cause de la géolocalisation des smartphones	17
Je ne pense pas que je changerai de comportement en ligne à cause du DPI	34	Je ne pense pas que je changerai de comportement à cause de la géolocalisation des smartphones	44
Je ne changerai pas de comportement en ligne à cause du DPI	18	Je ne changerai pas de comportement à cause de la géolocalisation des smartphones	25
Sans réponses	3	Sans réponses	6
Total	100	Total	100

Figure 23: Esquive active des technologies

participants ont supposé que le besoin souvent exprimé de pouvoir effacer des données personnelles dans des systèmes établis tient au malaise de se sentir constamment exposé au public.

7.5. Education et informations

Le besoin de contrôle et de transparence, ainsi que la question de pouvoir adapter son comportement, correspondent à l'aspiration à l'éducation et à l'information. L'appel à clarification est particulièrement vif en relation avec la jeune génération qui, de l'avis de nombre de participantes et participants, fréquenterait les médias électroniques de façon trop naïve et insouciante et serait même en partie dépendante de ces derniers.

Une personne s'est exprimée en ces termes : «Je pense que la sensibilisation est d'une grande importance, chacun doit savoir ce qu'il fait» Et une autre de relever : «Auparavant, j'étais mal informé, je me suis mis au courant avec la brochure. Ceci déjà est important – de savoir que cela se fait, de savoir aussi qui le fait et jusqu'où ça va. Cette information est la première chose que l'on devrait demander.»

Des exigences en ce sens ont été adressées aussi à l'école : «L'école devrait sensibiliser à ces questions, une heure d'enseignement devrait être dédiée à ce sujet ; il faudrait de surcroît des cours pour les adultes»

7.6. Améliorer le monde

Bien que l'objet déclaré des discussions de SurPRISE ait été les technologies de surveillance, dans tous les forums de discussion nombre de participantes et participants ont rappelé que la technique n'est pas toute la vie et qu'en définitive nous tous – la société – décidons comment les applications techniques sont utilisées et quelles conséquences il en résulte pour la communauté. La déclaration suivante est représentative de ce point de vue : «La technologie n'est pas la meilleure solution pour augmenter la sécurité. Il faut plutôt répartir la richesse et l'éducation. Il est plus bénéfique d'investir en peace building qu'en sécurité.»

De ce point de vue, les problèmes de sécurité ne peuvent pas uniquement être résolus par la technique – du moins pas si l'on aspire à davantage qu'à une simple lutte contre des symptômes. «On est énormément de gens dans le monde, et on pense que la protection, respectivement la sécurité, va nous sauver. Cela est un choix de société. Mais on aurait peut-être aussi pu faire un autre choix», a déclaré une personnes. Une carte postale écrite par quelqu'un de Zurich est représentative de déclarations similaires : «Ce ne sont PAS des technologies de pointe qui font naître le sentiment de sécurité ! Les grands problèmes de sécurité doivent être abordés sur une base BEAUCOUP plus large : la pauvreté, les courants migratoires, l'éducation pour tous les enfants, y compris les filles. Ce sera seulement quand les PREMIÈRES RELATIONS seront stables et affectueuses pour tous les enfants de la planète qu'une confiance originelle GLOBALE pourra se développer.»

7.7. Bilan de quelques hypothèses

Lors de la préparation des forums de discussion, les partenaires du projet SurPRISE ont développé en collaboration internationale une série d'hypothèses sur les facteurs censés influencer les attitudes à l'égard de la surveillance. Considéré dans son ensemble, l'échantillon suisse a confirmé beaucoup de ces suppositions.

Une des hypothèses centrales part de l'idée que des personnes qui se sentent personnellement en sécurité manifestent peu de sympathie vis-à-vis des technologies de surveillance. Les résultats des enquêtes et des discussions qui ont eu lieu en Suisse valident cette relation. Les gens se sentent très sûrs dans notre pays, en tout cas nettement plus sûrs que la moyenne de tous les pays partenaires. En même temps, les technologies

de sécurité en général, et notamment le DPI et – dans une mesure un peu moindre – la géolocalisation par le biais des téléphones portables, se heurtent à un rejet relativement fort. Ceci confirme la relation supposée entre un sentiment prononcé de sécurité personnelle et le scepticisme à l'égard des technologies de surveillance. Cette interaction peut être même démontrée à l'intérieur de la Suisse. Les réserves à l'égard des technologies de sécurité sont les plus faibles au Tessin, où le sentiment de sécurité personnelle semble être le moins prononcé. Par contre, c'est à Zurich, où les personnes questionnées se sentent le plus sûres, que ces technologies jouissent de l'acceptation la plus faible.L'hypothèse de travail centrale, selon laquelle les personnes qui sont particulièrement soucieuses de leur sphère privée sont aussi particulièrement hostiles aux techniques de surveillance est également confirmée par les résultats suisses. Car c'est en Suisse alémanique, où l'on se fait le plus de souci pour la sphère privée, que la surveillance affronte la plus forte opposition. Inversement, l'aversion contre les instruments étatiques de surveillance et de contrôle est la plus faible au Tessin où la préoccupation pour la sphère privée est comparativement la plus faible.

Une autre hypothèse est que l'image des institutions influence l'attitude de la population à l'égard de la surveillance technique. Elle suppose que la population se montre d'autant mieux disposée à l'égard des technologies de surveillance que les autorités paraissent plus crédibles, compétentes et proches des citoyens. Or elle est démentie par les résultats de la Suisse. Ici, les autorités obtiennent de meilleures notes qu'en moyenne de tous les pays participants, et ceci aussi bien en ce qui concerne la crédibilité que la sollicitude à l'égard des citoyennes et citoyens. Et néanmoins, on n'accueille pas favorablement la surveillance dans ce pays – même si cette dernière est exercée par des autorités perçues comme bienveillantes. Le sentiment de sécurité personnelle semble donc avoir plus de poids que la confiance à l'égard des autorités qui recourent à des technologies de surveillance.

Cependant, il est aisément concevable de supposer une relation entre les deux variables «sentiment de sécurité» et «perception des autorités». Le fait que beaucoup de gens se sentent à l'abri et chez eux dans notre pays pourrait tenir à une organisation étatique perçue grosso modo comme efficace, crédible et bienveillante. Dans un tel contexte, la surveillance technique se présente dans le meilleur des cas comme superflue, et dans les pires circonstances comme menaçante, parce qu'elle rappelle l'interdépendance mondiale, à laquelle on ne peut pas échapper complètement, même pas dans le confort local.

7.8. Ne pas mettre la confiance en jeu

Tant les résultats des enquêtes quantitatives que ceux des discussions mettent en évidence à quel point il importe d'utiliser les technologies de surveillance de façon appropriée et dans un cadre juridique clairement défini. La transparence est indispensable à cet égard : les gens veulent savoir quelles données sont recueillies, qui en est responsable et quels buts sont visés.

En Suisse, où les menaces sur la sécurité sont perçues moins fortement que dans d'autres pays, des mesures de surveillance intense, pénétrant trop profondément dans la sphère privée, pourraient se heurter rapidement à une opposition considérable. Et les autorités, qui jouissent d'une bonne réputation dans notre pays, risqueraient alors de perdre leur capital de confiance.

Car différentes opinions exprimées lors des discussions attestent que le scandale des fiches, à la fin des années 1980, est loin d'être oublié. Le Conseil fédéral est certes parvenu à rétablir la réputation des autorités en réorganisant les services de renseignement et en soumettant la surveillance à un cadre juridique strict. Sauvegarder cette confiance restaurée est une tâche très

exigeante, surtout dans une époque de rapide évolution technique et de grande instabilité de la situation en termes de menaces, où il s'agit de trouver un équilibre entre la protection de la sécurité nationale et la préservation de la sphère privée. Les débats actuels autour la révision de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) et de la loi sur le renseignement (LRens) attestent en tout cas que le recours à des technologies de sécurité recèle un grand potentiel de conflit. Sur cet arrière-plan, il est particulièrement important de renforcer la protection des données et de doter les services compétents des moyens nécessaires pour assumer leur tâche. On répondrait ainsi à une préoccupation centrale des citoyennes et citoyens, à savoir : garder le contrôle de ses propres données.

8. Table des illustrations

9. Annexes

9.1. Modèle

Template for recommendation round

Quelle est l'affirmation principale de la recommandation de votre table ?

Quel est le contexte de cette recommandation ? // Quel est le problème ?

Votre recommandation. // Que faire ? / Comment le problème peut-it être résolu ?

surprise

9.2. Recommandations Zürich (08.03.2014)

Quelle est l'affirmation principale de la recommandation de votre table ?	Quel est le contexte de cette recommandation?//Quel est le problème ?	Votre recommandation// Que faire?// Comment le problème peut-il être résolu?
La saisie des données doit être transparente, contrôlée et réglementée de façon définitive (s'applique à toutes les institutions qui récoltent des données).	Une utilisation des technologies de sécurité qui préserve le plus possible la sphère privée, pas d'accession aux données sans consentement. Manque de transparence à propos de qui enregistre, utilise et transmet des données à des tiers. Disproportion des atteintes à la sphère privée par rapport à d'autres domaines : p.ex. don d'organes (pas d'obtention de données sans consentement).	• Catalogue de critères qui définit clairement qui a le droit de récolter et utiliser quelles données pour une affectation déterminée. • Utilisation de meilleures technologies de cryptage (pare-feu) • Développement de technologies de sécurité de substitution • Lutte contre les causes de menaces de la sécurité, prévention.
Protéger la sphère privée aussi dans le secteur numérique.	Analyser de façon plus précise le réseau de lois. Rendre compte des données.	Qu'il soit plus difficile aux entreprises de changer les conditions d'utilisation. Protection des données sous le contrôle d'une autorité étatique forte.
On ne voit pas qu'il y ait transparence à propos de quelles données peuvent être récoltées sur nous quand, où et pour quelle raison.	L'utilisation de l'DPI conduit la société à une situation où il n'y a plus de présomption d'innocence. Tout comportement peut être mal interprété.	Nous exigeons davantage de transparence. Les fournisseurs de services doivent informer activement leurs clients : indiquer où ceux-ci sont enregistrés et quelles données à leur sujet sont enregistrées. Ces données doivent pouvoir être effacées après un certain laps de temps. Nous demandons que tous les citoyens et citoyennes de toutes les classes d'âge soient informés activement et sensibilisés au sujet des risques et dangers des médias électroniques. L'éducation aux médias doit être activement promue. Les citoyennes et citoyens doivent savoir comment se défendre et à qui ils peuvent s'adresser.
Transparence par l'information.	La non-transparence et l'impossibilité du contrôle par les individus.	Davantage de moyens pour l'éducation et la recherche destinées à améliorer la protection de la sphère privée des citoyens. Elaboration d'une charte internationale comprenant des normes applicables de façon générale. Création d'une instance suprême de surveillance, veillant au respect de ces normes. Droit fondamental de consultation de ses données personnelles.

Créer des conditions de transparence.	Méfiance, inconscience, ignorance, sous-estimation en ce qui concerne la saisie et l'utilisation des données.	• Créer des directives légales strictes. • Améliorer le contrôle/les organes de contrôle (contrôle du contrôle). • Créer des conditions uniformes au niveau national/européen. • Renforcer la prise de conscience par l'information de la population. • Assurer que les données ne puissent pas être manipulées.
Protection de la sphère privée	Le citoyen est trop peu maître de l'utilisation de ses données. L'Etat adopte un rôle trop passif en matière de protection de ses citoyens.	Il incombe à l'Etat d'assumer un rôle actif pour protéger les citoyens, et autant que possible assurer leur anonymat, en matière d'enregistrement des données. L'exploitation commerciale et privée de ces dernières doit être interdite. L'Etat doit élaborer à cet effet des lois claires et applicables.
Améliorer la protection de la sphère privée grâce à davantage de transparence : possibilités d'information. Séparer sécurité et commerce.	• L'utilisation abusive des données et le manque de sécurité qui en découle. • La législation est à la traîne en raison du développement fulgurant des nouveaux médias.	• La transmission des données à des tiers ne doit pas être partie intégrante des conditions générales. • Les utilisateurs doivent pouvoir déterminer quelles données peuvent être diffusées à des fins commerciales. • Les fournisseurs suisses de services doivent effacer complètement les données après un certain laps de temps. • La Confédération a l'obligation de s'investir pour la sensibilisation aux nouveaux médias dans les écoles et bien sûr aussi dans la population tout entière.
Informer, sensibiliser, autonomiser	La législation ne suit pas l'évolution technologique. L'utilisateur est tiraillé entre curiosité et risque. Conséquences du déterminisme technologique difficiles à évaluer.	Campagne d'information par les autorités, les écoles, les médias et les services spécialisés. Conditions politiques permettant de renforcer la position des utilisateurs par des technologies préservant mieux la vie privée («Privacy enhancing technologies»), des modèles «opt-in» et l'équilibrage entre les considérations de politique sécuritaire, d'ordre économique et de protection de la personnalité.
Qui renonce à sa liberté pour plus de sécurité perd finalement les deux.	Nous ne sommes pas convaincus de l'utilité des nouvelles technologies en matière de sécurité.	Les droits de l'homme, la protection des données et la transparence doivent avoir plus de poids que la satisfaction de besoins de sécurité.

Davantage de transparence pour ce qui a trait à la vie privée.	Manque de confiance en la société/à l'égard des institutions.	Autodétermination en ce qui concerne l'utilisation de nos données et de la technologie. L'évolution au sein de la société doit être abordée par la prévention/ la coopération. Résoudre ensemble les problèmes.
	L'DPI ne doit être utilisée que partiellement. Il faut protéger surtout le point terminal du transfert de données.	Soumettre l'utilisation de l'DPI à des conditions cadres juridiques strictes, qui garantissent que • seule une autorité étatique recourt à l'DPI • cette autorité est contrôlée par une instance politique.
Directives mondiales contraignantes pour la protection de la sphère privée, mettant l'accent sur les technologies d'information et de communication.	• La question de la protection de la sphère privée contre des technologies « modernes » ne peut plus être résolue au niveau national • Mise en réseau internationale de la technologie (aujourd'hui et à l'avenir).	• Elaboration d'une charte • Préposé mondial à la protection des données • Instauration d'une cour de justice, en analogie avec un tribunal pénal de l'ONU • Pour la Suisse : Créer les conditions cadres pour un intranet national (CH comme PME) afin d'assurer la protection contre un accès international aux données (p.ex. par Google) : un intranet conforme à la législation nationale, car sans « boucles » faisant transiter des données à l'étranger. (Remarque : pas de censure, 2 réseaux 1x CH-Intranet, 1x www = le choix est laissé aux citoyens)
Création de bases légales	• On ne sait pas qui est surveillé, combien de temps, pourquoi. • Quelles données peuvent être saisies et par qui n'est pas clair. • Ignorance au sujet des appareils de surveillance : lesquels existent sur le marché et à quelle fin peuvent-ils être utilisés ? • De quelle façon / dans quelle mesure les droits fondamentaux constitutionnels sont-ils menacés ?	• Les droits fondamentaux ayant trait à la sphère privée doivent être garantis. • Transparence au sujet de l'utilisation des données et de leur transfert à des tiers. • Contrôles indépendants assurés par des organes compétents. • Règlementation conviviale / information sur les conditions d'utilisation → consommatrices, consommateurs Rendre possible le contrôle de l'utilisation de leurs données. • Possibilité d'effacer des données : qui peut décider ? • Possibilités de consulter ses données

9.3. Recommandations Grandson (22.03.2014)

Quelle est l'affirmation principale de la recommandation de votre table ?	Quel est le contexte de cette recommandation?//Quel est le problème ?	Votre recommandation// Que faire?// Comment le problème peut-il être résolu?
Création d'une charte ou d'un label qualité garantissant les droits fondamentaux sur Internet (DPI)	Violation des droits de la vie privée, manque de transparence sur l'utilisation des données, absence d'aide à la décision. En particulier sur les sites type : Facebook, Twitter, boîte mail etc.	Que les sites adhèrent à une chartre délivrant un label qualité, géré par un organisme international indépendant et de confiance, existant ou à créer. Exemple des sujets compris dans la chartre : • Information continue sur l'évolution générale (technologies, législation) • Transparence sur l'utilisation des données • Limitation de l'utilisation des données au maximum • Interdiction d'effectuer des modifications de contenus (liste non exhaustive)
Nous apprécions les nouvelles technologies avec comme souci principale la protection de la sphère privée	Manque de maîtrise et de transparence des données utilisées. Les données ne sont pas utilisées uniquement pour la protection des personnes	Axer sur la formation pour toutes les classes de la population. Standardisation des conditions d'utilisation
Réglementer le DPI et la géolocalisation de façon à ce que la liberté individuelle soit respectée, au niveau européen	Obtenir le consentement complet du consommateur/utilisateur	Prévoir un code législatif, prévoir un organe de contrôle par état de préservation de la liberté individuelle, sensibilisation et information des populations
Garantir l'éthique, le débat démocratique	Respect des droits humains (liberté religieuse, politique, sexuelle, respect de la sphère privée), qui ne sont pas toujours respectés, absence de débat public, opacité.	Garantir la transparence sur l'accès et l'utilisation des données récoltées, les garder sans contrôle démocratique dans le respect des droits humains. Résolution : légiférer (niveau national et international).
Mise en place d'un cadre légal au niveau européen qui respecte les droits fondamentaux de l'individu.	Manque de clarté législative. Rapidité de l'évolution technologique. Manque de cohérence. Mondialisation du «réseau».	Information des citoyens sur les résultats obtenus suite à l'utilisation des technologies de sécurité. Information/ formation dans l'éducation obligatoire. Imposer un cadre aux entreprises privées qui utilisent les technologies de sécurité notamment en ce qui concerne la clarté des conditions d'utilisation.
Consultation citoyenne (sur les sujets importants discutés) plus régulière et plus complète.	Le vide législatif sur le DPI et les géolocalisations. L'insuffisance de l'information sur le DPI surtout auprès des jeunes.	Légiférer nationalement ou internationalement. Limiter la lecture des DPI en interdisant la manipulation du DPI, sauf en cas de questions juridiques et sécurité nationale. Améliorer l'information du citoyen sur tous les problèmes. Commission éthique informatique.

Renforcer la législation actuelle afin de faire de la vie privée une priorité concernant ces technologies (au niveau Suisse et européen).	Perte de maîtrise des outils et des données due à l'évolution des technologies. L'évolution des technologies se fait au détriment de la vie privée. Dépendance des consommateurs dues au peu de fournisseurs (manque d'alternative)	Favoriser l'indépendance des consommateurs (élargir l'offre). Limiter la capture des données en renforçant la loi. Développer l'information et l'éducation sur ces technologies pour protéger la vie privée de l'utilisateur. Réaffiner les principes fondamentaux qui définissent les droits de la vie privée (inclure le droit de prescription pour la sauvegarde des données).
Il faut donner une priorité élevée à la protection de la sphère privée dans une perspective de sauvegarde de la démocratie et des droits fondamentaux des personnes.	L'apparition de nouvelles technologies présentent des opportunités et des risques. En revanche les personnes manquent d'informations et d'outils afin de maîtriser ces technologies et leurs manipulations et, afin d'opérer des choix éclairés.	Elaboration d'un cadre légal, qui impliquera : • Une obligation à l'information et l'éducation • Obligation à la transparence sur qui utilise quelles infos à quelles fins • Obligation de protéger le cadre d'utilisation des données individuelles par des tiers • Poser des limites à l'utilisation des données individuelles et en assurer le contrôle. • Garantir le choix à l'utilisateur sur le type de données qui sont transmissibles (GPS, accès à la caméra).
Encadrement strict de l'utilisation des données DPI et géolocalisation	DPI : Accès aux données à trop d'acteurs privés et commerciaux. Géolocalisation : absence de choix de l'activation ou pas	DPI : Créer un cadre légal limitant son utilisation à la sécurité étatique sous contrôle judiciaire et parlementaire. Interdiction de l'utilisation à des fins commerciales et privées. Géolocalisation : Portrait des conditions générales de l'activation automatique de la géolocalisation et de l'utilisation par des tiers. Non transmission des données et réversibilité de l'accord. En général : Accès pour tout citoyen à l'information d'utilisation de ses données.
Délimiter les clauses de sécurité, leurs conditions d'utilisation et de conduite démocratique. Garantir le droit à la préservation de la sphère privée : c'est-à-dire droit à l'information, au consentement et au libre choix.	On doute de l'argument de vente «sécurité» : quelle sécurité ? pour qui ? pour quoi ?. Le public en général est tenu dans l'ignorance de ce qui est réellement fait de ces données personnelles.	Qui contrôle qui ? Pourquoi ?
Manque de transparence : s'engager dans la transparence et dans l'information de la procédure de l'utilisation des données collectées	-	Et la création d'un réseau européen et création d'une charte d'éthique d'utilisation de ces données.

La nécessité d'améliorer la transparence, le contrôle et l'utilisation des données enregistrées	L'inquiétude et le doute quant à l'utilisation de ces données et à leur recoupement dans un but autre que la sécurité nationale (commerciale, données sur la santé, RH).	Affiner la loi actuelle de protection des données. Mettre sur pied une entité de contrôle nationale et européenne. Renforcer la prévention éducationnelle. Pousser l'autonomisation de l'Europe face aux USA.
La criminalité est due au manque d'éducation, à la mauvaise répartition des richesses, qui créent un sentiment d'insécurité.	La technologie n'est pas la meilleure solution pour promouvoir la sécurité.	Pour augmenter la sécurité, il ne faut pas mettre l'accent sur la traque des criminels, mais se donner les moyens de faire en sorte qu'il y en aie moins. Utiliser d'avantage de moyens pour la répartition des biens, l'éducation etc. Prévention et anticipation, d'avantage de transparence. Il y a plus de bénéfices à travailler sur la paix que sur la sécurité. Peace building.

9.4. Recommandations Lugano (29.03.2014)

Quelle est l'affirmation principale de la recommandation de votre table ?	Quel est le contexte de cette recommandation?//Quel est le problème ?	Votre recommandation// Que faire?// Comment le problème peut-il être résolu?
Information, transparence, bases légales de portée générale, prévention, dépendance	• Information : prise de conscience et connaissance des avantages et inconvénients des moyens utilisés • Transparence : les utilisateurs ne sont absolument pas informés sur l'utilisation de leurs données • Bases légales : des lois et standards applicables au niveau international font défaut • Prévention : l'ampleur de la récolte de données n'est pas assez connue	• Mise en œuvre de lois valables pour tous et appliquées par toutes les nations • Information et éclaircissements sur l'ampleur des données et sur le potentiel technologique des moyens employés, notamment pour les mineurs (branche scolaire) • L'utilisateur doit avoir le droit de savoir ce qui est fait des informations qui le concernent et d'obtenir un feed-back à ce sujet. • « Permis de conduire » pour le smartphone • Il faut chercher activement des voies de substitution pour assurer la protection de la sécurité nationale • Programmes de resocialisation et de sevrage pour les utilisateurs souffrant d'addiction au smartphone.
Limitation de la vie privée au nom d'une sécurité commune prétendue plus grande.	La soi-disant « nécessité » d'augmenter la sécurité.	Bases légales plus claires (DPI et géolocalisation) Mise au courant des citoyens/utilisateurs Formation aux médias pour les citoyens/citoyennes et les services de contrôle Institution d'un organe de contrôle aux compétences bien définies
Nous exigeons des normes légales claires et univoques.	Le fait que le recours à ces moyens technologiques n'est pas organisé de façon transparente nous préoccupe.	Nous exigeons que chaque utilisateur de telles technologies doive expressément et obligatoirement donner son consentement en ce qui concerne l'utilisation et la réutilisation de ses propres données. Il faut des lois claires, appliquées dans le monde entier, visant à une utilisation transparente ; la diffusion des données doit être limitée et ces dernières doivent être effacées après un laps de temps clairement défini. Peines sévères pour les violations de la sphère privée des individus et de la société. Surveillance des surveillants.

Des règles claires pour un recours proportionné aux technologies de sécurité.	Empêcher les abus en matière de droit de la personnalité.	Création d'une organisation internationale neutre pour surveiller le développement technologique et garantir un libre accès à des informations indépendantes. Il faut en outre davantage de transparence sur qui récolte et conserve des données sensibles.
Améliorer la prise de conscience et augmenter la protection par des mesures au niveau politique.		Veiller à ce que l'information de la population ne donne pas aux aspects technologiques plus de poids qu'aux aspects sociaux et à ce qu'elle prenne en compte aussi les risques. Il doit y avoir des sanctions claires et efficaces pour tous ceux qui récoltent ou utilisent des données personnelles de façon illicite.
Créer des lois et des règles. Mais aussi davantage de transparence.	Il manque des informations claires sur les risques que courent les utilisateurs de ces technologies. En même temps, les bases légales sont insuffisantes ou font totalement défaut ; les lois doivent être harmonisées au niveau national aussi bien qu'international.	Créer des lois et des organes de contrôle indépendants. Faire connaître qui gère les services (internet) et définir clairement quelles sont les tâches et les responsabilités de ces personnes. Les utilisateurs doivent être en tout temps informés de façon transparente sur les risques et sur leurs droits. La technologie doit être indépendante du service qui l'utilise. L'utilisateur doit pouvoir déterminer quand et comment des atteintes aux droits et notamment à sa sphère privée sont admissibles.
Transparence, information, éducation	Manque de connaissances sur la question de savoir comment les données sont saisies, gérées, évaluées, et dans quel but elles sont utilisées.	Transparence : simplifier les dispositions juridiques (cc) concernant les nouvelles technologies. Rendre public qui se sert des données. Information : informer plus en détail et plus fréquemment par le biais de différents canaux de communication. Education : éducation à l'école, sensibilisation et introduction d'une période d'enseignement consacrée à ces questions, et aussi des cours pour adultes.
Les droits de la personnalité et la sphère privée sont inaliénables.	Les objectifs visés par ces technologies sont sans aucune mesure avec les violations qui en résultent de la sphère privée et de la liberté individuelle.	Nous exigeons des politiciens un engagement commun en faveur d'une réglementation claire qui définisse exactement comment l'DPI et la localisation par les téléphones portables sont utilisées, contrôlées et si nécessaire limitées, de manière à ne pas porter atteinte au droit à la sphère privée.
Améliorer l'information pour renforcer la prise de conscience des utilisateurs sur les conséquences du recours à ces technologies.	Nous constatons que les données d'utilisateur sont utilisées dans des buts qui représentent une atteinte à la sphère privée ou même une agression.	Nous exigeons des politiciens : • qu'une information relative aux risques de l'utilisation de la télématique soit partie intégrante de l'enseignement scolaire ; • que les fabricants des appareils et les fournisseurs de services aient l'obligation d'informer brièvement et clairement les consommateurs sur les risques qu'ils courent en ce qui concerne leur sécurité personnelle.

Manque d'information, manque de protection contre un abus de ces technologies. Nécessité urgente d'une meilleure information sur la question de savoir quelles technologies sont déjà appliquées.	Menace sur la vie privée. Prise de conscience insuffisante quant aux implications de l'utilisation des technologies, à l'espionnage, à la commercialisation, à l'utilisation illicite de données personnelles.	Campagne de sensibilisation pour toutes les classes d'âge. Bases légales et normes communes à l'échelon européen, peines sévères en cas d'abus, obligation de donner son consentement (privacy by design). Les données personnelles doivent être gérées par l'Etat, option d'adhésion obligatoire pour les buts commerciaux.
Information et éducation dès l'enfance, pour que tout ce qui a affaire à la surveillance, à la sécurité et à la sphère privée soit rendu transparent.	La complexité d'une question qui concerne tout un chacun et qui doit être mieux expliquée et être réglementée de façon plus explicite au niveau international.	• Information et éducation sur la question dès le début de la scolarité. • Les autorités de protection des données doivent fournir en permanence à la population des informations accessibles à tous au sujet des technologies de sécurité (possibilité de discuter et poser des questions). • Harmonisation des règles internationales par des institutions telles que l'ONU ou l'UIT, qui siègent déjà en Suisse. • Les fabricants des appareils doivent avoir l'obligation de donner aux utilisateurs la possibilité d'activer et désactiver certains mécanismes de surveillance.
Il faut créer une réglementation de portée mondiale (dont le champ d'application s'étende aussi au-delà de l'Europe), fixant comment des données personnelles saisies et récoltées par des technologies de sécurité peuvent être utilisées et examinant sous un angle critique l'intérêt et l'efficacité de leur utilisation à des fins de sécurité.	• Ces technologies sont très intrusives et il est impossible de contrôler qui s'en sert et comment. • Les problèmes (terrorisme) que ces technologies sont censées résoudre sont présentées comme plus graves qu'ils ne sont en réalité. La question se pose de savoir s'il est vraiment nécessaire d'y recourir. • Il existe des doutes quant à l'efficacité réelle de ces technologies. Des solutions de substitution (le facteur humain) seraient préférables.	• Légiférer/réglementer au niveau mondial (à grande échelle) pour protéger la sphère privée en relation avec le recours à ces technologies et avec les données qu'elles saisissent. • Estimer clairement la nécessité effective de recourir à ces technologies. Evaluer la menace et les risques de façon proche de la réalité et recourir aux technologies de sécurité avec la retenue qui s'impose. Des solutions de substitution doivent être recherchées, et en matière de sécurité il faut accorder plus d'importance au facteur humain (autorités chargées d'enquêter) qu'à la technologie. • La population doit être informée correctement sur ces technologies, leur utilisation et leurs risques, et ceci déjà à l'âge préscolaire. Cette information doit la rendre capable de se protéger contre certains risques et de faire une approche consciente de ces technologies.

9.5. Partenaires du projet

Partenaires du projet SurPRISE

- Institut für Technikfolgen-Abschätzung/Österreichische Akademie der Wissenschaften, Cordinateur du projet, Autriche (ITA/ÖAW).
- Agencia de Protección de Datos de la Comunidad de Madrid*, Espagne (APDCM).
- Instituto de Politicas y Bienes Publicos/Agencia Estatal Consejo Superior de Investigaciones Científicas, Espagne (CSIC).
- Teknologirådet - The Danish Board of Technology Foundation, Danemark (DBT).
- European University Institute, Italie (EUI).
- Verein für Rechts-und Kriminalsoziologie, Autriche (IRKS).
- Medián Opinion and Market Research Limited Company, Hongrie (Median).
- Teknologirådet - The Norwegian Board of Technology, Norvège (NBT).
- The Open University, Royaume-Uni (OU).
- Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein/Allemagne (ULD).

* APDCM, die Agencia de Protección de Datos de la Comunidad de Madrid (autorité de la protection des données de la ville de Madrid) était partenaire du projet SurPRISE jusqu'au 31 décembre 2012. En raison de la situation politique régnant en Espagne, la collaboration a pris fin en décembre 2012.

Groupe de conseil

- Bruno Baeriswyl, Préposé cantonal à la protection des données, Comité directeur de TA-SWIS, Zürich.
- Sami Coll, chercheur associé, Département de sociologie, Université de Genève.
- Francisco Klauser, Institut de géographie, Université de Neuchâtel.
- Katharina Prelicz-Huber, Présidente Vpod, Comité directeur de TA-SWISS, Zürich.
- Philipp Stüssi, service du Préposé fédéral à la protection des données, Berne.

Direction du projet

- Sergio Bellucci, TA-SWISS, Berne.
- Danielle Bütschi, TA-SWISS, Berne.
- Dilini-Sylvie Jeanneret, TA-SWISS, Berne.

Secrétariat

Helen Curty, TA-SWISS, Berne.

Modération

Zurich, 08.03.2014

Modération principale: Haas Josefa, directrice de l'école cantonale de formation continue (EB), Zürich.
Modération de table et prise de note: Serdal Avsar, Sergio Bellucci, Patrick Beutler, Ursina Biasio, Sebastian Büchler, Alexandra Erne, Urs Gerber, Helena Neuhaus Wettstein, Sarina Reichlin, Lucienne Rey, Christina Tobler, Linda Toffolon, Ursina Wey, Alessandra Willi.

Grandson, 22.03.2014

Modération principale: Xavier De Stoppani, Altercoaching, Genève.
Modération de table et prise de note: Claire Bellmann, Nadia Besnard, Nadia Ben Zbir, Christine D'Anna-Huber, Myriam Ernst, Roberto Finocchio, Pascale Gerber, Claude-Evelyne Guillaume, Florence Hügi, Dilini-Sylvie Jeanneret, Claudie Leconte, Didier Mermillion, Lucienne Rey, Delphine Wolf.

Lugano, 29.03.2014

Modération principale: Giovanni Pellegri, Ideaotorio, Université de la Suisse italienne.
Modération de table et prise de note: Elena Casabianca, Janos Cont, Christine D'Anna-Huber, Laura Ferrario, Peter Giada, Lisa Giuppomi, Francesca Massei, Sebastiano Mazzola, Fabio Meliciani, Luca Mennella, Marisa Mengotti, Giona Morinini, Lucienne Rey, Martina Zilioli.

SurPRISE est un projet de recherche financé par la Commission européenne, dans le cadre de son septième programme-cadre.

TA-SWISS
Centre d'évaluation des choix technologiques
Brunngasse 36
CH-3011 Berne
info@ta-swiss.ch
www.ta-swiss.ch

Un centre de compétence des
Académies suisses des sciences

Rapport TA-P18/2014