Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Affaire Crypto AG

Rapport de la Délégation des Commissions de gestion des Chambres fédérales du 2 novembre 2020

Avis du Conseil fédéral

du 26 mai 2021

Monsieur le Président,
Madame, Monsieur,

Conformément à l'art. 158 de la loi sur le Parlement, nous nous prononçons comme suit sur le rapport du 2 novembre 2020 de la Délégation des Commissions de gestion des Chambres fédérales concernant l'affaire Crypto AG.[1]

Nous vous prions d'agréer, Monsieur le Président, Madame, Monsieur, l'assurance de notre haute considération.

26 mai 2021

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Guy Parmelin
Le chancelier de la Confédération, Walter Thurnherr

1 FF **2021** 156

Avis

1 Contexte

Le 10 novembre 2020, la Délégation des Commissions de gestion des Chambres fédérales (DélCdG) a transmis son rapport sur l'affaire Crypto AG au Conseil fédéral, en le priant de prendre position sur ses observations et recommandations avant le 1er juin 2021 au plus tard.

«L'affaire Crypto AG» désigne une opération du renseignement trouvant son origine dans les années 1970, lorsque l'entreprise Crypto AG, dont le siège se trouvait en Suisse, est passée entre les mains communes des services de renseignement américains et du service de renseignement allemand. Dès 1993, le Service de renseignement stratégique (SRS) a appris que la société Crypto AG exportait des appareils «vulnérables», dont le chiffrement comportait des failles. Lorsque le SRS a été transformé en une unité administrative civile en 2001, il a réussi, grâce à une collaboration avec les services de renseignement américains, à acquérir un certain nombre d'informations sur l'étranger à l'aide de tels appareils de l'entreprise Crypto AG.

L'enquête de la DélCdG a démontré qu'aucun des prédécesseurs du chef actuel du DDPS n'avait été informé de cette opération par les chefs ou directeurs du Service de renseignement de la Confédération (SRC) ou de l'une des organisations antérieures. La responsable du DDPS a pour la première fois été sommairement informée par le directeur du SRC le 19 août 2019 des aspects critiques entourant la société Crypto AG. Le directeur du SRC a alors reçu le mandat de rechercher des informations consolidées sur cette affaire. Par la suite, elle a été informée de manière plus détaillée le 31 octobre 2019 de l'intérêt médiatique suscité par l'entreprise ainsi que des conséquences éventuelles des révélations se rapportant à la collaboration en matière de renseignement. La raison de l'intérêt médiatique résidait dans la publication annoncée d'un rapport secret («MINERVA – A History») des services de renseignement américains sur l'opération consacrée à Crypto AG.

Début novembre 2019, la responsable du DDPS a informé le Conseil fédéral, qui s'est ensuite intéressé de très près à l'affaire Crypto AG. Le présent avis revient une nouvelle fois sur la chronologie exacte de toutes les activités du DDPS, des autres départements ainsi que de la Chancellerie fédérale et du Conseil fédéral.

Le DDPS a informé le Conseil fédéral des premières constatations se rapportant à l'affaire Crypto AG lors de la séance du Conseil fédéral du 6 novembre 2019, au moyen d'une note d'information secrète. Le 7 novembre 2019, une réunion a eu lieu avec la responsable du DDPS, le vice-chancelier et porte-parole du Conseil fédéral, le secrétaire général du DDPS, la secrétaire générale du DFJP et des représentants du SRC, lors de laquelle il a été décidé de créer un groupe de travail interdépartemental et d'informer les autorités de surveillance (DélCdG et Autorité de surveillance indépendante des activités de renseignement, AS-Rens). Le président de la DélCdG et le chef de l'AS-Rens ont été informés en personne par la responsable du DDPS sur le contenu de la note secrète le 12 novembre 2019. La première séance du groupe de

travail interdépartemental a eu lieu le 18 novembre 2019. Cinq séances au total ont eu lieu jusqu'au 3 mars 2020.

L'affaire Crypto AG a été traitée lors de la séance du Conseil fédéral du 20 décembre 2019 sur la base d'une note de discussion du DDPS. À cette occasion, le Conseil fédéral a décidé de la marche à suivre, chargeant le DDPS de lui remettre à la séance du 15 janvier 2020 une proposition pour la conduite d'un organe d'enquête indépendant, élaborée conjointement avec le DFJP. Le 8 janvier 2020, l'ancien juge fédéral Niklaus Oberholzer a été sollicité par le secrétaire général du DDPS pour savoir s'il serait disposé à enquêter sur les circonstances entourant l'affaire Crypto AG. Il s'est déclaré prêt à accepter ce mandat.

Le 20 décembre 2019, le SECO a révoqué les licences générales ordinaires d'exportation pour deux sociétés qui ont succédé à Crypto AG, à savoir TCG Legacy AG et Crypto International AG, et les a suspendues *sine die*. Cette décision a été prise sur instruction de la direction du DEFR. À cette occasion, il a également été décidé que le SECO continuerait à traiter des demandes d'exportation individuelles.

Le 15 janvier 2020, sur proposition du DDPS, le Conseil fédéral a confié à Niklaus Oberholzer la conduite de l'organe d'enquête chargé d'examiner les circonstances ayant entouré l'affaire Crypto AG. Il lui a été octroyé un accès rapide à tous les documents pertinents conservés aux Archives fédérales suisses (AFS) et dans les unités administratives concernées. Il devait remettre un premier rapport au Conseil fédéral à la fin juin 2020 au plus tard. S'il s'avérait alors que le mandat d'enquête exigeait d'être précisé après un premier examen des documents existants, le DDPS en informerait le Conseil fédéral.

Il a par ailleurs été décidé que le rapport d'enquête serait présenté au Conseil fédéral à la fin juin 2020. Sur la base des premières conclusions tirées à ce moment-là, le Conseil fédéral déciderait alors de la marche à suivre et d'un éventuel approfondissement de l'enquête. Niklaus Oberholzer a commencé ses travaux le 16 janvier 2020 aux AFS.

Le 14 février 2020, la DélCdG a informé le Conseil fédéral par écrit qu'elle avait ouvert une inspection formelle. Simultanément, elle saluait l'enquête commandée par le Conseil fédéral et l'autorisait à poursuivre ces travaux, conformément à l'art. 154*a*, al. 1, de la loi sur le Parlement (LParl; RS *171.10*).

La responsable du DDPS a reçu le 15 février 2020 un premier rapport succinct du Niklaus Oberholzer sur ses premières investigations. Le Conseil fédéral a pris acte de ce document le 19 février 2020, sur la base d'une note d'information secrète du DDPS.

Considérant que cela était dans l'intérêt d'un examen rapide et efficace, la DélCdG a décidé à la fin février 2020 que l'enquête diligentée par le Conseil fédéral et confiée à Niklaus Oberholzer devait se poursuivre sous sa responsabilité avec effet immédiat. De la sorte, toutes les investigations effectuées jusqu'alors sur l'affaire Crypto AG se retrouvaient intégrées à l'inspection de la DélCdG. Cette dernière a communiqué sa décision au Conseil fédéral le 21 février 2020 et en a informé la presse le 26 février 2020.

Le 25 février 2020, le SECO a déposé une plainte pénale contre inconnu auprès du Ministère public de la Confédération (MPC), la justifiant par une probable violation de la législation sur le contrôle des biens.

Le 5 mars 2020, la présidente de la Confédération a informé par écrit la DélCdG que le Conseil fédéral avait pris connaissance de la décision de cette dernière de révoquer l'autorisation de poursuivre l'enquête conférée à Niklaus Oberholzer. Dans ce courrier, le Conseil fédéral s'engageait à assurer le bon déroulement du transfert du dossier et à soutenir la délégation dans son enquête. Jusqu'au terme de l'inspection menée par la DélCdG, soit début octobre 2020, les départements et offices concernés ont fourni à la DélCdG un grand nombre de documents. Des membres du Conseil fédéral et des représentants de l'administration fédérale ont participé à plusieurs auditions de la DélCdG.

Le 19 juin 2020, le Conseil fédéral a décidé, sur proposition du DEFR, de suspendre la décision sur les demandes d'exportation individuelles de l'entreprise «Crypto International AG» jusqu'au terme de l'enquête menée par le MPC. Le Conseil fédéral a même confirmé cette décision le 26 août 2020, en réponse à une demande de reconsidération déposée par la société.

Le 7 octobre 2020, la DélCdG a transmis au Conseil fédéral pour avis le projet de rapport sur son inspection. Le Conseil fédéral a ensuite fait parvenir à la DélCdG son avis du 28 octobre 2020, accompagné du contrôle correspondant des faits. Le rapport définitif de la DélCdG sur l'affaire Crypto AG a été publié le 10 novembre 2020.

2 Avis du Conseil fédéral

2.1 Généralités

Comme il a été décrit précédemment, plusieurs départements et le Conseil fédéral lui-même se sont intéressés de très près à l'affaire Crypto AG. Le Conseil fédéral rejette dès lors la critique exprimée par la DélCdG selon laquelle il n'aurait pas reconnu la «portée politique» de l'affaire. Les informations données immédiatement par le DDPS au Conseil fédéral, l'examen détaillé du cas auquel le Conseil fédéral a procédé, la mise sur pied d'un groupe de travail interdépartemental et le mandat confié à Niklaus Oberholzer attestent du sérieux avec lequel le cas a été traité et sont la preuve que le Conseil fédéral était fermement décidé à faire toute la lumière sur cette affaire. La DélCdG l'a d'ailleurs reconnu dans son courrier adressé au Conseil fédéral le 14 février 2020, avant de décider une semaine plus tard, le 21 février 2020, de révoquer son autorisation d'enquêter et de reprendre la direction des enquêtes sur l'affaire Crypto AG.

Le Conseil fédéral comprend la volonté de placer l'enquête sous une direction unique, car ce choix est pertinent du point de vue et de la méthodologie et du contenu. En revanche, il est difficile pour lui de comprendre les raisons pour lesquelles la DélCdG, en février 2020, a changé d'avis en l'espace d'une semaine.

Deux rapports ont été établis sur l'affaire Crypto AG: le rapport de la DélCdG du 2 novembre 2020 et un rapport classé secret rédigé par Niklaus Oberholzer sur mandat

de la DélCdG. Pour des questions de confidentialité, la DélCdG n'a pas souhaité remettre le rapport Oberholzer au Conseil fédéral. La DélCdG a proposé au Conseil fédéral de lui donner accès au rapport secret Oberholzer selon une procédure analogue à celle que prévoit l'art. 167, al. 3, LParl, donc de réserver cet accès à la conseillère fédérale en charge du SRC. Par courrier du 6 novembre 2020, le Conseil fédéral a informé la DélCdG qu'il renonçait à consulter le rapport Oberholzer classé secret si ce droit n'était pas étendu à tous les membres du Conseil fédéral, au chancelier de la Confédération et au directeur du SRC. Aux yeux du Conseil fédéral, la procédure proposée par la DélCdG empêche de se prononcer en connaissance de cause sur l'ensemble des conclusions de la délégation (rapport de la DélCdG et rapport Oberholzer). Aussi le Conseil fédéral ne se prononce-t-il dès lors ici que sur le rapport de la DélCdG.

2.2 Concernant les aspects liés au renseignement

S'agissant du volet de l'affaire Crypto AG ressortissant à proprement parler au renseignement, le Conseil fédéral constate que l'activité des services de renseignement SRS et SRC était conforme au droit, comme en a attesté la DélCdG, que ce soit dans un premier temps sur la base de la loi sur l'armée et l'administration militaire (LAAM, RS *510.10*), puis sur la base de la loi sur le renseignement (LRens, RS *121*). Le Conseil fédéral est par ailleurs d'accord avec l'appréciation de la DélCdG selon laquelle la recherche d'informations liée à cette activité a eu une utilité avérée au fil des ans. Il s'agit de tenir compte de cette évaluation dans l'appréciation de la «portée politique» s'agissant de la dimension du renseignement.

Ce qui est problématique, comme l'a observé la DélCdG, c'est que les accès existants aux informations de Crypto AG étaient un secret bien gardé au sein de la direction de l'ancien SRS. Elles sont restées la chasse gardée de ce petit cercle de personnes. C'est la raison pour laquelle la direction politique du renseignement n'a pendant longtemps pas été informée, même au temps du SRC. Il faut enfin constater que la DélCdG elle-même n'a jamais été informée de l'opération par le service de renseignement depuis 1993 et qu'elle n'avait donc aucune connaissance de cette affaire jusqu'à ce que la responsable du DDPS l'en informe en novembre 2019. Le Conseil fédéral partage l'avis de la DélCdG selon lequel une information aurait dû lui être donnée en l'espèce par le service de renseignement.

Après que la responsable du DDPS eut reçu des informations confirmées sur cette affaire de la part du directeur en exercice du SRC, elle en a informé le Conseil fédéral et les organes de surveillance (DélCdG et AS-Rens). Le Conseil fédéral est en outre d'avis que les événements n'ont pas été évalués de façon équitable par la DélCdG. Il estime en effet que le rapport de la DélCdG aurait dû porter la même appréciation sur l'ensemble des directeurs qui avaient eu connaissance de l'opération et qui n'en ont pas informé les dirigeants politiques.

D'un point de vue juridique, il est tout à fait admissible aux yeux de la DélCdG que le SRC et un service étranger utilisent conjointement une société en Suisse pour rechercher des informations sur l'étranger. Dans un tel cas de figure, le Conseil fédéral partage l'appréciation de la DélCdG selon laquelle le service de renseignement doit

en informer les autorités politiques, afin que celles-ci puissent en analyser les éventuelles conséquences sur le plan de la sécurité, de la politique étrangère ou de la politique économique. Quant à la question de savoir si l'affaire Crypto AG est problématique du point de vue du droit de la neutralité, le Conseil fédéral renvoie à la réponse qu'il a donnée à l'interpellation Molina 20.4456: «L'art. 9 de la Convention de La Haye de 1907 ne s'applique pas au cas présent, car les faits ne relèvent pas de limites imposées à des États ou d'interdictions à l'égard de parties belligérantes. Le Conseil fédéral ne voit donc en l'occurrence aucune violation à la Convention de La Haye.»

Le Conseil fédéral constate par ailleurs que l'affaire Crypto AG n'a en rien gêné la politique étrangère de la Suisse ni porté atteinte à sa crédibilité. Il n'y a quasiment pas eu de réactions d'États tiers vis-à-vis de la Suisse suite au rapport précité.

2.3 Concernant les licences d'exportation

Le Conseil fédéral rejette ici les reproches selon lesquels il aurait usé de manœuvres dilatoires et aurait eu l'intention d'éviter un rapport défavorable.

Après avoir pris connaissance des problèmes liés aux chiffrements possiblement manipulés des appareils de la société Crypto AG, le chef du DEFR a ordonné comme mesure immédiate la révocation de la licence générale ordinaire d'exportation. Grâce à la révocation du 20 décembre 2019 par le SECO, il a été possible d'empêcher que des exportations aient lieu sans contrôles préalables. Des demandes d'exportation individuelles ont quant à elles pu continuer à être déposées.

Le SECO aurait à tout moment été disposé à rendre très rapidement une décision susceptible de recours, pour autant qu'une demande ait été déposée en ce sens. Or, à aucun moment, les entreprises concernées par la révocation et représentées par des avocats n'ont demandé que soit rendue une telle décision. Comme l'illustrent bien les plaintes déposées auprès du Tribunal administratif fédéral contre la suspension prononcée par le SECO des demandes d'exportation déposées, les entreprises en question ont certainement examiné la possibilité de faire usage d'une voie de droit.

Le Conseil fédéral ne partage pas l'avis de la DélCdG selon lequel la révocation de la licence générale ordinaire d'exportation aurait été contraire au droit. Il n'y a en effet aucun droit à bénéficier de l'octroi d'une licence générale ordinaire d'exportation. Le permis peut être octroyé, comme l'observe aussi la DélCdG, lorsque les exigences de la loi sur le contrôle des biens (LCB; RS *946.202*) et de l'ordonnance sur le contrôle des biens (OCB; RS *946.202.1*) sont remplies. L'art. 7, al. 2, LCB dispose que les permis peuvent être retirés si les conditions qui y sont liées et les charges dont ils sont assortis ne sont plus observées. Dans le cas présent, la révocation n'est pas due uniquement aux raisons mentionnées à l'art. 6 LCB motivant le refus d'octroyer des permis d'exportation.

Le DEFR et le SECO disposaient à l'époque d'informations qui justifiaient des doutes sérieux quant à la possibilité pour les entreprises concernées de pouvoir prouver qu'elles avaient mis en place un contrôle interne fiable visant à faire respecter les prescriptions en matière de contrôle à l'exportation, tel que l'exige l'art. 5, al. 2, OCB. Par conséquent, à ce moment-là, il n'était ni arbitraire ni contraire au droit de révoquer

les licences générales ordinaires d'exportation, compte tenu des éléments factuels dont disposait le DEFR. Cette procédure était d'autant plus justifiée qu'il restait possible d'octroyer des permis d'exportation individuels, tout en permettant dans le même temps un contrôle des biens à exporter. La suspension par le Conseil fédéral des permis d'exportation individuels jusqu'au terme de l'enquête pénale menée par le MPC constituait la dernière étape d'une procédure d'autorisation au cours de laquelle des réserves avaient déjà été préalablement émises au sein du groupe interdépartemental de contrôle des exportations lors de l'examen des demandes d'exportation individuelles.

Selon les art. 12 et 13 OCB, l'octroi de licences générales d'exportation est de la seule compétence du SECO. Il est donc déplacé de faire le reproche d'une absence d'implication du groupe interdépartemental de contrôle des exportations.

2.4 Concernant la plainte pénale

Loin de déposer la plainte pénale à la légère, le SECO a procédé en amont et dans la mesure du possible aux clarifications nécessaires et rassemblé toutes les informations disponibles.

Le reproche selon lequel la plainte pénale aurait été déposée pour des motifs politiques est infondé. Sur la base des éléments factuels dont il disposait, le SECO s'est senti légalement tenu de faire part de ses soupçons de possibles actes délictueux en déposant une plainte pénale auprès du MPC. De fait, le SECO a déposé cette plainte parce qu'il soupçonnait que les demandes reçues pour l'exportation d'appareils de chiffrement contenaient des données incorrectes, ce qui aurait constitué un délit au sens de l'art. 14, al. 1, let. a, LCB. La plainte pénale a par ailleurs mis en avant une possible violation de l'art. 9, al. 1, let. a, de l'ordonnance sur l'exportation et le courtage de biens destinés à la surveillance d'Internet et des communications mobiles (OSIC; RS *946.202.3*), en raison là aussi d'indications incorrectes ou incomplètes dans les demandes d'exportation.

Après le dépôt et l'examen de la plainte pénale déposée par le SECO, la Police judiciaire fédérale a saisi sur ordre du MPC quelque 400 appareils des entreprises Crypto International AG et TCG Legacy. Dans sa demande d'autorisation adressée au Conseil fédéral, le MPC a expliqué qu'il y avait un soupçon suffisant de délit ou de crime selon les art. 14 LCB et 9 OSIC. Comme en témoignent les mesures conservatoires prises, le MPC non seulement partageait les soupçons du SECO, mais reconnaissait dans sa demande d'autorisation l'existence d'une présomption suffisante d'infraction. Cette réalité bat en brèche le reproche selon lequel la plainte pénale aurait été juridiquement infondée.

Le MPC a par ailleurs répété dans ses considérations sur l'ordonnance de non-lieu qu'il soupçonnait l'existence d'actes délictueux. Dans son appréciation juridique de l'ordonnance de non-lieu, le MPC a expliqué qu'il supposait que des appareils exportés de la société Crypto AG étaient dotés de points faibles, que le chiffrement de communications étrangères pouvait être déchiffré par des services secrets initiés et que l'usage à des fins de renseignement des appareils de chiffrement exportés faisait partie d'une collaboration entre le SRS, puis plus tard le SRC, avec des services secrets

étrangers. Depuis 2002, les bases légales autorisant une telle collaboration étaient suffisantes, celle-ci s'étant du reste déroulée sans sortir du cadre légal.

À aucun moment, le DEFR et le SECO n'ont disposé d'informations qui leur auraient permis de vérifier si les soupçons allégués étaient justifiés par des motifs juridiquement pertinents.

3 Concernant les recommandations

Le Conseil fédéral se prononce comme suit sur les recommandations de la DélCdG:

Recommandation 1

La cheffe du DDPS et son Secrétariat général se dotent des instruments nécessaires pour être à même, d'une part, de se procurer immédiatement et de manière autonome les informations dont ils ont besoin si une affaire liée au renseignement survient et, d'autre part, de veiller à ce que la conduite politique du SRC et la capacité d'action du Conseil fédéral soient assurées. Tant que cela n'est pas garanti, les mandats confiés à l'AS-Rens ou à des chargés d'enquête externes ne doivent pas être considérés comme opportuns.

Le Conseil fédéral n'est pas d'accord avec cette recommandation.

Le pilotage politique du SRC par le DDPS et le Conseil fédéral est clairement réglé dans plusieurs bases légales (voir en particulier les art. 70 et 80 LRens). Selon l'art. 19 de l'ordonnance sur le Service de renseignement (ORens; RS *121.1*), le SRC doit fournir chaque année un rapport au chef du DDPS sur tous les opérations et informateurs. D'après cette disposition, le SRC aurait dû impérativement informer le DDPS sur l'activité qu'il menait en lien avec la société Crypto AG, qui impliquait une collaboration avec un service partenaire étranger.

Les séances mensuelles organisées avec la direction du SRC font aussi partie du dispositif de contrôle du service de renseignement dont dispose le chef du DDPS. Depuis janvier 2014, ces séances font l'objet de procès-verbaux, qui ont été remis à la DélCdG pour son inspection. Les activités opérationnelles du SRC sont régulièrement au menu de ces séances.

Dans l'affaire Crypto AG, le problème n'était pas le manque d'instruments de contrôle au niveau du DDPS ou du Conseil fédéral, mais l'intention de collaborateurs du SRS puis du SRC de tenir l'opération secrète et de la soustraire au contrôle politique. Il s'agissait en l'espèce d'une opération au long cours, dont les circonstances et les conséquences possibles n'étaient pas faciles à appréhender.

Dans une telle situation, un examen par l'AS-Rens constituerait une mesure raisonnable. L'AS-Rens est certes un organe de contrôle indépendant, mais le DDPS est parfaitement habilité à lui proposer d'engager des investigations sur un sujet particulier. Dans l'affaire Crypto AG, l'AS-Rens a par exemple procédé à une inspection inopinée des locaux d'archivage du SRC, avec l'autorisation de la DélCdG.

En revanche, la DélCdG a refusé que l'AS-Rens mène une inspection sur la légalité des activités opérationnelles du SRC en collaboration avec le Centre des opérations électroniques (COE), comme le proposait le DDPS. Le Conseil fédéral ne partage pas l'appréciation de la DélCdG à cet égard. Il aurait été pertinent de s'adresser à l'AS-Rens en cette affaire, d'autant qu'un tel recours s'inscrit dans le cadre du mandat légal de l'autorité de surveillance (voir l'art. 78, al. 1, LRens), à quoi s'ajoute que l'AS-Rens aurait été disposée à intégrer cette enquête dans sa planification annuelle 2020.

S'agissant de cette enquête par l'AS-Rens, la DélCdG écrit que le DDPS aurait dû demander l'autorisation de la délégation, conformément à l'art. 154*a*, al. 1, LParl. Or, cette disposition ne concerne expressément que les enquêtes disciplinaires ou administratives. Or, on peut se demander si une enquête de l'AS-Rens entre dans l'une ou l'autre de ces catégories.

Au sein du SG DDPS, les moyens humains du conseil en matière de renseignement au profit du chef du DDPS ont été renforcés depuis janvier 2021. Cette évolution n'est en rien liée au traitement de l'affaire Crypto AG, mais découle des expériences faites ces dernières années ainsi que des tâches supplémentaires liées à l'entrée en vigueur de la LRens. Il s'agit ici avant tout de l'appréciation et de la validation des nouvelles mesures de recherche d'informations soumises à autorisation du SRC.

Recommandation 2

Le DDPS fait appel à la Délséc de manière ciblée pour garantir l'échange d'informations au sujet de dossiers dans le domaine du renseignement et ainsi renforcer la capacité de conduite du Conseil fédéral lors d'affaires liées au renseignement. La Délséc ou une délégation ad hoc du Conseil fédéral doit en particulier intervenir lorsque le DDPS ne souhaite ou ne peut pas communiquer des informations secrètes au sein d'organes de l'administration.

Pour le Conseil fédéral, cette recommandation est déjà mise en œuvre.

La Délégation du Conseil fédéral pour la sécurité (Délséc) s'intéresse régulièrement et de manière approfondie aux questions liées au renseignement. Les thèmes ressortissant au renseignement constituent une part importante des affaires traitées par la Délséc, comme en attestent les ordres du jour et procès-verbaux des séances de la Délséc, que la DélCdG reçoit également.

Le Conseil fédéral ne partage pas l'avis de la DélCdG selon lequel un organe ad hoc supplémentaire serait utile pour améliorer l'aptitude à la conduite du Conseil fédéral. Dans l'affaire Crypto AG, le problème principal ne résidait pas dans le fait que le DDPS aurait fait de la rétention d'informations vis-à-vis du Conseil fédéral, mais dans le fait que le service de renseignement avait omis jusqu'en 2019 d'informer la direction politique et les autorités de surveillance. Les informations auxquelles le service de renseignement avait accès concernant la société Crypto AG étaient un secret bien gardé au sein de la direction de l'ancien SRS et n'étaient réservés qu'à ce cercle étroit de personnes. La création d'organes supplémentaires au sein de l'administration ou au niveau du Conseil fédéral n'apporterait aucune amélioration dans une telle situation.

Recommandation 3

Le DDPS s'assure que le CdA participe en général aux séances de la Délséc en qualité de représentant de l'administration. Si la préparation des dossiers de la Délséc l'exige, le CdA participe aussi aux séances du Groupe Sécurité.

Le Conseil fédéral est partiellement d'accord avec la recommandation.

La Délséc est une délégation du Conseil fédéral et donc un organe politique. Elle est constituée des trois chefs des départements du DDPS, du DFAE et du DFJP, la présidence en étant assurée par le chef du DDPS. Les trois membres de la Délséc peuvent se faire accompagner par des collaborateurs de leurs départements. En règle générale, il s'agit des membres du Groupe Sécurité, qui prépare de nombreux dossiers de la Délséc, ainsi que des secrétaires généraux. Les membres de la Délséc sont libres, selon le thème abordé, de convoquer d'autres personnes à leurs séances, ce qui arrive régulièrement. Cela peut aussi être le chef de l'Armée (CdA), lorsque le sujet concerne l'armée. Prévoir une participation permanente du CdA à la Délséc n'aurait toutefois guère de sens, les thèmes ayant trait à l'armée n'étant abordés qu'exceptionnellement.

Recommandation 4

Si une collaboration en matière de renseignement entre le SRC et un service étranger implique une entreprise suisse, le DDPS en informe le Conseil fédéral. Le Conseil fédéral fixe les critères selon lesquels il statuera lui-même sur une telle collaboration.

Le Conseil fédéral est partiellement d'accord avec la recommandation.

Le Conseil fédéral estime que la recommandation de la DélCdG va dans le bon sens. Il considère cependant que devoir d'information et compétence décisionnelle réservée en matière d'activités de renseignement ne devraient pas être limités aux cas qui concernent des entreprises suisses et dans lesquels le service de renseignement collabore avec des partenaires étrangers. D'autres activités ressortissant au renseignement peuvent en effet revêtir une importance politique majeure. Ce qui est déterminant, c'est que le service de renseignement informe qui de droit de manière précoce par la voie de service, afin que la direction politique puisse assumer sa fonction de conduite et de surveillance. Le principal facteur déclencheur d'une information doit par conséquent être la possible dimension politique d'une opération. L'implication d'une entreprise suisse constitue certes un indicateur à cet égard, mais non le seul critère déterminant. Suivre des affaires où des entreprises suisses sont simplement impliquées, comme dans le cadre de flux usuels de paiements auprès de banques, ou participer à l'observation coordonnée à l'échelle internationale de possibles activités de prolifération par des entreprises suisses, fait partie des tâches habituelles d'un service de renseignement. De telles affaires ne devraient remonter à l'échelon gouvernemental que si elles recèlent des chances ou des risques majeurs d'un point de vue politique.

Le DDPS informe aujourd'hui déjà le Conseil fédéral sur les activités et observations importantes relevant du renseignement. Le Conseil fédéral souhaiterait dès lors

accepter la recommandation sous une forme plus générale et définir pour ce faire des critères permettant de déterminer les activités ressortissant au renseignement dont il souhaite être informé par le DDPS et les conditions dans lesquelles il veut lui-même autoriser de telles activités. Ces critères peuvent être élaborés dans le cadre de la révision de la LRens et de l'ORens avant d'y être inscrits.

La LRens ne confère cependant aucune compétence décisionnelle d'ordre opérationnel au Conseil fédéral en matière de renseignement. L'art. 70 LRens réglemente avant tout le pilotage politique et la surveillance par le Conseil fédéral. L'art. 70, al. 1, let. e, LRens dispose toutefois que le Conseil fédéral ordonne les mesures nécessaires en cas de menaces particulières. L'art. 12*a* de la loi sur l'organisation du gouvernement et de l'administration (LOGA; RS *172.010*) précise par ailleurs que les départements informent régulièrement le Conseil fédéral sur leurs dossiers, notamment sur les risques et les difficultés qu'ils peuvent présenter, et que le Conseil fédéral peut exiger de ses membres certaines informations. L'art. 38 LOGA affirme le droit des chefs de département d'intervenir personnellement dans les décisions des unités administratives qui leur sont subordonnées. L'art. 13 LOGA est certes avant tout une prescription procédurale, mais donne une indication sur le fait que c'est le Conseil fédéral qui prend les décisions d'importance majeure ou qui ont une portée politique particulière. Les normes existantes permettent dès lors aujourd'hui déjà au Conseil fédéral de prendre des décisions de portée politique en matière de renseignement.

Le Conseil fédéral est d'accord avec la DélCdG pour considérer que le service de renseignement doit informer les responsables politiques sur les opérations dont la portée est comparable à celle de l'affaire Crypto AG. Au cours des dix dernières années, les obligations du SRC de rendre compte des opérations de renseignement ont été systématisées et étendues. Les activités concernant la société Crypto AG n'ont toutefois jamais fait l'objet d'un tel compte rendu, parce que, comme il a été dit précédemment, les informations concernant Crypto AG auxquelles certains avaient accès étaient le secret bien gardé d'un petit nombre de personnes au sein de la direction du SRS puis du SRC, et qu'elles sont restées réservées à ce petit cercle de personnes.

Recommandation 5

La Confédération ne fait pas l'acquisition de solutions de cryptage auprès de fournisseurs étrangers. Les fournisseurs indigènes doivent garantir à la Confédération qu'ils ont le contrôle des aspects liés à la sécurité du développement et de la production..

Le Conseil fédéral met en œuvre cette recommandation dans la mesure du possible.

Appréciation générale d'un point de vue pratique

Au sein de l'administration fédérale, le chiffrement est partout, par exemple dans les téléphones mobiles utilisés à des fins professionnelles (iPhone). Contrôler l'entreprise Apple sur ce plan n'est pas possible. Cette seule raison explique déjà pourquoi la recommandation n'est pas intégralement réalisable. Ensuite, non seulement toutes les solutions de chiffrement utilisées actuellement pour les échelons de classification À USAGE INTERNE et CONFIDENTIEL proviennent de fournisseurs étrangers, mais

la recommandation est problématique sur le plan de l'interopérabilité. L'interopérabilité des systèmes de chiffrement multifactoriels aujourd'hui répandus est en effet incompatible avec une telle recommandation. De plus, les solutions suisses de chiffrement propriétaires n'apportent presque aucun avantage par rapport à des solutions de chiffrement en libre accès (*open source*). Quant à la validation de l'implémentation en bonne et due forme de la technologie de chiffrement concernée, elle doit de toute manière être garantie pour les deux solutions. Globalement, d'un point de vue pratique, cette recommandation semble dès lors difficilement réalisable. On retrouve aujourd'hui des solutions de chiffrement dans de nombreux systèmes et composants. Dans les faits, cette recommandation signifierait qu'aucun logiciel ne pourrait plus être acheté à l'étranger.

En revanche, si la recommandation vise des services-clés, à l'instar de ceux du DFJP (p. ex. dans le secteur de la criminalité organisée), du DFAE (pour le réseau extérieur) ou du DDPS (notamment pour le SRC), alors une mise en œuvre semble globalement réaliste.

Il faut toutefois remarquer que les fournisseurs suisses ne peuvent pas eux non plus garantir à 100 % qu'ils contrôlent tous les aspects de sécurité du développement et de la fabrication. Ces entreprises suisses n'en offrent pas moins des avantages indéniables en comparaison avec les entreprises étrangères, concernant par exemple la nécessaire déclaration de sécurité de l'entreprise ou encore le contrôle de sécurité relatif aux personnes. Ces avantages déploient avant tout leurs effets en cas de collaboration de longue durée.

Il existe par ailleurs en Suisse des fournisseurs certes intéressants aussi pour Armasuisse, mais qui ont des filiales dans d'autres pays. Or, dans certains de ces pays, des lois obligent les fabricants à coopérer avec les services de l'État (p. ex. le *Patriot Act* aux États-Unis ou des lois analogues en Chine et en France). Par conséquent, une collaboration avec une entreprise suisse ayant des filiales à l'étranger peut être tout aussi problématique du point de vue de la politique de sécurité.

Appréciation d'un point de vue juridique

Du point de vue du droit des marchés publics, la recommandation peut être mise en œuvre. La loi révisée du 21 juin 2019 sur les marchés publics (LMP; RS *172.056.1*), entrée en vigueur le 1er janvier 2021, prévoit que le droit des marchés publics ne s'applique pas aux marchés publics «dont l'exemption est jugée nécessaire pour la protection et le maintien de la sécurité extérieure ou intérieure ou de l'ordre public» (art. 10, al. 4, let. a, LMP). La Confédération peut par conséquent à tout moment attribuer un marché de gré à gré en Suisse pour l'acquisition de solutions de chiffrement.

D'un autre côté, la Confédération ne peut influer sur l'offre proposée par les prestataires de services. À l'heure actuelle, il n'existe qu'une seule entreprise suisse qui propose des solutions de chiffrement. Or, lorsque la Confédération s'approvisionne auprès d'un fournisseur unique sur le marché, celui-ci acquiert une position de monopole. Le droit des marchés publics prévoit des instruments de contrôle pour de tels cas de figure, notamment la conclusion d'un droit d'accès à la comptabilité de l'entreprise ainsi que des droits d'audit. Il ne faut cependant pas perdre de vue qu'une situation de monopole n'empêche pas un risque de faillite, de destruction économique

de l'entreprise et donc de perte de savoir-faire. De même, il n'est pas possible d'empêcher contractuellement la vente d'actions pour prévenir un transfert de propriété d'une entreprise à l'étranger.

Afin de pouvoir mettre en oeuvre cette recommandation, il faudrait par conséquent faire en sorte que l'entreprise en question reste liée à la Confédération au-delà de la prestation contractuelle à fournir. S'agissant des contrats de services et des projets de recherche, il faudrait par ailleurs veiller à ce que les droits immatériels restent entre les mains de la Confédération. Les instruments à cet effet sont connus, parmi lesquels: PPP[2], contrats de coopération, mise en commun de la R&D, etc. Vu les expériences faites par le passé, il faut néanmoins s'attendre à ce que de telles mesures renchérissent les acquisitions concernées. La dépendance économique de la Confédération vis-à-vis de l'entreprise en question peut en revanche être amoindrie.

Concernant les aspects relevant de la politique de sécurité

Outre les aspects juridiques et pratiques, il y a également lieu de tenir compte des aspects relevant de la politique de sécurité, avant tout sous l'angle de la base technologique et industrielle importante pour la sécurité (BTIS).

Sur sa liste des technologies importantes pour la sécurité[3], le domaine Sciences et technologies d'Armasuisse considère la cryptologie comme une «technologie-clé importante pour la sécurité». La cryptologie est une technologie-clé non seulement pour la Suisse mais pour le monde entier. Dans le monde actuel, numérique et interconnecté, tous les mécanismes électroniques de sécurité ou presque se fondent sur des procédures cryptographiques. Les opérations bancaires en ligne, le commerce électronique, la cyberadministration et tous les autres services électroniques seraient inimaginables sans la cryptographie. Avec la généralisation du numérique, elle va par ailleurs encore gagner en importance, tant pour l'économie et la société que pour les autorités. Dans ses principes en matière de politique d'armement du DDPS, le Conseil fédéral réaffirme la nécessité de renforcer les compétences technologiques importantes pour la sécurité et les capacités industrielles essentielles dans le cadre de la BTIS.

Ce qui précède est également développé et confirmé dans le rapport de la DélCdG. La compétence technologique en Suisse se trouve aujourd'hui en particulier auprès du Service de cryptologie (BAC/crypt) de la Base d'aide au commandement de l'armée, mais aussi auprès du domaine Sciences et technologies d'Armasuisse. La compétence d'acquérir des systèmes cryptologiques en toute sécurité se trouve chez Armasuisse. Au-delà de ces compétences propres à la Confédération, il importe de trouver des partenaires industriels hautement qualifiés. Et si ces derniers se trouvent à l'étranger, il n'est presque pas possible d'influer sur le développement de tels appareils. L'affaire Crypto AG illustre bien les risques et les conséquences possibles pour les États qui doivent se procurer de tels systèmes auprès d'un fournisseur à l'étranger.

2 Partenariats public-privé (PPP).

3 La liste comprend 213 technologies qui ont été classées par degrés de priorité selon les besoins de l'armée. Les technologies auxquelles a été attribué le degré de priorité le plus élevé sont considérées comme des technologies-clés importantes pour la sécurité.

Dans ce contexte, il s'agirait d'analyser de plus près les possibilités offertes par la loi fédérale sur les entreprises d'armement de la Confédération (LEAC, RS *934.21*), par exemple en termes de prise de participation à des entreprises. Ces possibilités pourraient ouvrir des pistes de solutions souples et praticables pour résoudre le problème de sécurité soulevé ici par la DélCdG.

Le Conseil fédéral a compris l'importance de telles compétences technologiques et capacités industrielles: c'est pourquoi il a précisé dans ses principes du 24 octobre 2018 en matière de politique d'armement du DDPS qu'il entend notamment préserver et renforcer dans le cadre de la BTIS les technologies-clés et les capacités industrielles essentielles.

Recommandation 6

Le DDPS veille à ce que l'armée conserve suffisamment de compétences spécialisées en matière de cryptologie pour pouvoir évaluer la sécurité des solutions de cryptage acquises par la Confédération. Il fait en sorte que les synergies entre les compétences en matière de cryptographie et de cryptanalyse soient exploitées de manière optimale.

Cette recommandation sera mise en œuvre.

Au vu des développements technologiques à venir, des défis liés à la généralisation du numérique et des besoins croissants en matière de sécurité, il sera indispensable de consolider les compétences techniques en matière de cryptologie. Afin de s'assurer les compétences nécessaires, il s'agira d'encourager des formes appropriées de partenariat et de collaboration, sans perdre de vue la nécessité de privilégier des solutions économiquement viables.

Recommandation 7

Le DDPS veille à ce que les capacités en cryptanalyse restent adaptées aux besoins existant dans le domaine de l'interception des communications, dont les possibilités ont été étendues à l'exploration du réseau câblé dans la LRens.

Cette recommandation sera mise en œuvre.

Afin que la cryptanalyse puisse s'adapter à ces évolutions, il faut d'une part des accès aux points faibles, pour pouvoir les comprendre et finalement aussi les utiliser à des fins de renseignement, et d'autre part un échange avec d'autres services spécialisés.

L'échange international avec d'autres services de renseignement revêt à cet égard une importance toute particulière. Conformément à l'art. 12, al. 3, LRens, le SRC est compétent pour la collaboration avec des services de renseignement étrangers à des fins d'exécution de la LRens (et donc aussi de l'exploration radio et l'exploration du réseau câblé). D'entente avec le COE, il définit donc chaque année sa stratégie en matière de services partenaires et par-là même celle en matière de cryptologie. Cette stratégie définit avec quels services partenaires étrangers et sur quels champs thématiques le COE et la cryptologie ont des échanges techniques réguliers. Le SRC vise

à ouvrir à la cryptologie les accès nécessaires aux services partenaires, à les préserver puis à les renforcer encore davantage à l'avenir.

Il faut par ailleurs signaler ici que les compétences cryptographiques et cryptanalytiques doivent être considérées dans leur globalité, car des solutions théoriquement inviolables sont elles aussi menacées.

Recommandation 8

Le DDPS règle comment la documentation de l'échelon le plus élevé de la direction se rapportant à son activité directe de conduite et de surveillance dans les affaires liées au renseignement doit être archivée de manière sûre et légale. En outre, le SG-DDPS assure l'archivage de la documentation personnelle des anciens chefs du département et rend des comptes à la DélCdG.

Le Conseil fédéral considère que cette recommandation a déjà été mise en œuvre. Le SG DDPS va rendre un rapport à la DélCdG sur sa réalisation.

Le SG DDPS tient et documente ses dossiers de manière systématique dans le système GEVER Acta Nova, conformément à la loi fédérale sur l'archivage (LAr; RS *152.1*). Conformément aux directives d'organisation applicables à la gestion de l'information au SG DDPS, le Centre de compétences GEVER (CC GEVER SG DDPS) vérifie chaque année dans le dispositif de classement du SG DDPS, conjointement avec les domaines responsables du SG DDPS, s'il est possible d'éliminer du système certains dossiers.

Les dossiers qui sont ou ont été considérés comme ayant une valeur archivistique sont remis aux AFS aux fins d'archivage. La transmission se fait électroniquement via le processus d'archivage standardisé des AFS. Les documents de travail personnels de la direction supérieure du département sont en règle générale proposés aux AFS aux fins d'archivage au terme de la période de fonction, conformément aux recommandations des AFS (aide-mémoire «Documents de travail personnels et archives privées de magistrats de la Confédération»). Il n'y a pas besoin de directives supplémentaires à cet égard.

Depuis janvier 2014, les réunions régulières entre le chef du DDPS et le directeur du SRC font l'objet d'un procès-verbal (voir plus haut l'avis concernant la recommandation 1). Ces documents sont traités conformément aux prescriptions précitées.

Recommandation 9

La DélCdG considère qu'il est nécessaire que le SRC puisse, en cas de besoin, accéder rapidement aux connaissances disponibles au sujet des activités de renseignement passées. À cette fin, le SRC établit une vue d'ensemble des opérations et des sources au sujet desquelles il existe encore des dossiers, ce en parallèle à l'archivage des documents issus de la recherche opérationnelle et des échanges menés entre les organisations qui l'ont précédé et des services étrangers.

Le Conseil fédéral est d'accord avec cette recommandation. Sa mise en œuvre pose toutefois quelques questions qui doivent être clarifiées.

Après la publication de cette recommandation de la DélCdG, le SRC a stoppé la livraison convenue avec les AFS pour février 2021 de dossiers opérationnels des organisations qui ont précédé le SRC, dont ceux se rapportant à la société Crypto AG, afin de ne pas nuire à la mise en œuvre de cette recommandation.

Selon l'art. 6 LAr, l'administration fédérale propose aux AFS des dossiers à archiver dont elle n'a plus besoin en permanence, donc qu'elle ne traite plus régulièrement. Des exceptions sont possibles lorsque l'unité administrative est elle-même responsable de l'archivage. Selon la LAr, cependant, le SRC remet ses documents pour archivage aux AFS, ce qui est confirmé à l'art. 68 LRens.

La législation sur les archives limite l'accès des services fournisseurs aux documents archivés contenant des données personnelles. Pendant le délai de protection, les services ayant livré des documents aux AFS ne peuvent les consulter que s'ils en ont besoin comme moyens de preuve, c'est-à-dire dans une procédure juridique, à des fins législatives ou jurisprudentielles, pour des évaluations à buts statistiques ou pour prendre une décision visant à autoriser, à restreindre ou à refuser le droit de la personne concernée de consulter les documents ou d'obtenir des renseignements (art. 14, al. 2, LAr). L'art. 68, al. 3, LRens confère par ailleurs un droit de consultation au SRC afin de lui permettre d'évaluer des menaces concrètes pour la sécurité intérieure ou extérieure ou de préserver un autre intérêt public prépondérant. L'accès du SRC à ses archives est donc garanti, mais uniquement dans le cadre des procédures prévues par les AFS.

La recommandation implique que le SRC établit des vues d'ensemble des dossiers à archiver et qu'il les conserve en sa possession, afin de pouvoir identifier rapidement s'il a archivé des documents concernant certaines affaires ou personnes. Ces vues d'ensemble peuvent être conservées au SRC plus longtemps que les documents auxquels elles se réfèrent, pour autant que le service en ait besoin régulièrement. Au cas où elles sont jugées présenter une valeur archivistique, ces vues d'ensemble devront elles aussi être transmises ultérieurement aux AFS. Une telle procédure est a priori possible, mais soulève néanmoins certaines questions, concernant par exemple les droits d'accès. Le SRC clarifiera ces questions avec les AFS.

Recommandation 10

La DélCdG invite le Conseil fédéral à révoquer l'autorisation qu'il a donnée pour la procédure pénale que le MPC a lancée sur la base de la plainte pénale déposée par le SECO. Ensuite, le DEFR devra fournir aux entreprises qui ont succédé à Crypto AG les autorisations d'exportation demandées pour lesquelles aucun motif juridique clair ne justifie un rejet.

Cette recommandation est caduque.

Par décision du 8 décembre 2020, le MPC a classé la procédure pénale ouverte pour violation des art. 14 LCB et 9 OSIC (art. 319, al. 1, let. b et c, du code de procédure pénale [CPP; RS *312.0*]).

Le Conseil fédéral a pris acte de la décision de classement du MPC le 29 décembre 2020 et chargé le SECO de réexaminer les demandes concernées par la décision du Conseil fédéral du 19 juin 2020 et de les autoriser, pour autant que les conditions

juridiques préalables soient réunies. Le 30 décembre 2020, le SECO a autorisé toutes les demandes pendantes (aussi bien celles qui avaient été suspendues à la suite de la décision du Conseil fédéral du 19 juin 2020 que les autres) des entreprises qui ont succédé à la société Crypto AG, émettant le lendemain de nouvelles licences générales d'exportation.

Recommandation 11

Les notes d'information secrètes concernant des affaires liées au renseignement ou ayant un rapport avec des affaires en cours d'examen par la DélCdG, et dont le Conseil fédéral a pris connaissance, sont communiquées au fur et à mesure à la DélCdG. Le Conseil fédéral soumet à la délégation une proposition concernant la procédure à suivre.

Cette recommandation sera mise en œuvre.

La Chancellerie fédérale va examiner conjointement avec le secrétariat de la DélCdG comment y répondre s'agissant notamment des «affaires ayant un rapport avec des affaires en cours d'examen par la DélCdG». Le Conseil fédéral soumettra ensuite une proposition de procédure à la DélCdG.

Recommandation 12

La DélCdG doit préalablement être consultée au sujet des plaintes pénales de la Confédération portant sur des affaires ou des personnes qui font l'objet d'une enquête menée par la délégation. À cette fin, le département compétent ou la ChF demande un avis écrit à l'autorité de poursuite pénale concernée.

Le Conseil fédéral estime que cette recommandation est juridiquement et matériellement problématique, et il la rejette en conséquence.

Le Conseil fédéral comprend la crainte de la DélCdG de voir certaines de ses enquêtes gênées ou retardées par des plaintes pénales déposées par des autorités fédérales et visant des procédures ou des personnes qui sont justement l'objet de ces enquêtes. Même si les enquêtes pénales menées par des autorités de poursuites pénales cantonales ou fédérales et l'exercice de tâches de surveillance par la DélCdG ne poursuivent pas nécessairement les mêmes objectifs (voir notamment l'art. 154*a*, al. 4, LParl, selon lequel une enquête de la DélCdG n'empêche pas l'engagement ou la poursuite d'une enquête pénale préliminaire ou d'une procédure pénale) et qu'elles ne doivent dès lors pas obligatoirement être synchronisées, il est également dans l'intérêt du Conseil fédéral que les procédures ne se parasitent pas les unes les autres.

Le Conseil fédéral est toutefois d'avis qu'un processus de consultation institutionnalisé, ou même prescrit par la loi, tel qu'il figure dans la première phrase de la recommandation 12, n'est ni nécessaire ni opportun, pour les raisons suivantes:

– Les procédures se rapportant à l'affaire Crypto AG sont sans équivalent. Le Conseil fédéral n'a pas connaissance d'un autre cas où une autorité de la Confédération aurait déposé une plainte pénale télescopant matériellement et temporellement une enquête de la DélCdG. Le rapport de la DélCdG n'identifie

pas lui non plus d'affaires qui devraient être écartées en raison de l'obligation de consultation prévue par la recommandation. En conséquence, le Conseil fédéral estime qu'il ne se justifie pas d'exciper de ce cas particulier pour en tirer une règle de procédure générale.

– Chacun a le droit a priori de déposer une plainte pénale (art. 301 CPP). Mais les autorités fédérales ont en outre parfois l'obligation de déposer plainte. Plusieurs lois fédérales, dont justement la LCB, prévoient en effet que les autorités d'autorisation ou de contrôle de la Confédération, mais également les organes de police des cantons et des communes ainsi que les autorités douanières, sont tenus de dénoncer au MPC les infractions à la loi «qu'ils ont découvertes ou dont ils ont eu connaissance dans l'exercice de leurs fonctions» (voir les art. 18, al. 2, LCB, mais aussi 40, al. 2, de la loi fédérale sur le matériel de guerre [LFMG; RS *514.51*], 100, al. 3, de la loi sur l'énergie nucléaire [LENu; RS *732.1*], 27, al. 2, de la loi fédérale sur les prestations de sécurité privées fournies à l'étranger [LPSP;RS *935.41*], ou encore 27*a* de la loi fédérale sur l'Assurance suisse contre les risques à l'exportation [LASRE;RS *946.19*). Lorsque les autorités fédérales sont tenues de dénoncer, il reste peu de place pour une consultation préalable dans les formes.

– L'obligation de consulter la DélCdG prévue par la recommandation impliquerait dans la pratique que l'administration fédérale soit informée systématiquement et précocement par la DélCdG des personnes et affaires qui sont sous enquête de la DélCdG, ce qui pourrait parfois contrevenir aux besoins des enquêtes de la DélCdG. Il s'agirait également de préciser les informations que l'autorité fédérale qui envisage de porter plainte devrait fournir à la DélCdG, afin que celle-ci puisse exercer judicieusement son droit d'être consulté. Enfin, si une action rapide était requise, ces processus pourraient être préjudiciables à l'efficacité tant des poursuites pénales que de la haute surveillance exercée par la DélCdG.

Dans la deuxième phrase de sa recommandation 12, la DélCdG propose que le département compétent ou la Chancellerie fédérale – entendant certainement par là le département, ou la Chancellerie fédérale, auquel appartient l'autorité fédérale (unité administrative) autorisée ou contrainte à déposer plainte – doive préalablement demander un avis à l'autorité de poursuite pénale avant de consulter la DélCdG. Outre le fait que cette étape procédurale supplémentaire pourrait ralentir tout le processus, une telle coordination avec les autorités de poursuite pénale ne semble pas souhaitable aux yeux du Conseil fédéral, pour des raisons de principe.

De manière générale, le droit de dénoncer prévu par la loi n'est pas assorti d'une réserve obligeant à demander d'abord à l'autorité de poursuite pénale si et comment celle-ci réagirait à une dénonciation. Une plainte pénale permet de porter à la connaissance de l'autorité pénale un comportement jugé répréhensible. L'autorité pénale doit alors examiner si le comportement dénoncé constitue véritablement une infraction et si d'autres conditions d'une poursuite pénale sont réunies. Plusieurs possibilités s'offrent à l'autorité de poursuite pénale au terme de cet examen. Elle peut par exemple décider de ne pas entrer en matière sur la plainte, notamment si les éléments constitutifs de l'infraction ou les conditions à l'ouverture de l'action pénale ne sont manifestement pas réunis (art. 310 CPP). Elle peut aussi suspendre l'instruction, notamment

lorsque l'issue de la procédure pénale dépend d'un autre procès dont il paraît indiqué d'attendre la fin (art. 314, al. 1, let. b, CPP). Elle peut enfin ouvrir une instruction ou renvoyer à la police pour complément d'enquête les rapports et dénonciations lorsque ceux-ci n'établissent pas clairement les soupçons retenus (art. 309, al. 1 et 2, CPP). Il apparaît ainsi qu'elle n'a pas à répondre au moment de la dénonciation pénale, et encore moins avant, à la question de savoir si et comment elle entend y réagir.

L'obligation exigée par la recommandation de demander d'abord l'avis de l'autorité de poursuite pénale reviendrait dans les faits à demander à cette même autorité de procéder elle-même à un examen préliminaire des conditions et de l'opportunité d'une poursuite pénale à engager par elle-même – une obligation à ce jour inconnue du code de procédure pénale suisse. Et même si un tel examen préliminaire devait être considéré comme judicieux, il ne manquerait pas de poser des questions aussi complexes qu'innombrables. Qu'en est-il de la préimplication juridiquement douteuse des personnes concernées par la procédure pénale au cas où plainte pénale serait effectivement déposée ensuite ? Dans quelle mesure le Conseil fédéral et l'administration fédérale seraient-ils liés à l'avis exprimé par l'autorité de poursuite pénale ? Enfin, quel serait le poids d'une telle consultation préalable dans le cas de délits poursuivis d'office, qui devraient ensuite être poursuivis par l'autorité de poursuite pénale de toute façon et indépendamment d'une éventuelle plainte pénale, ne serait-ce qu'en raison des informations fournies par les autorités fédérales ? Pour toutes ces raisons, le Conseil fédéral considère qu'il n'est ni nécessaire ni opportun de creuser l'idée d'une telle consultation préalable.