Dritte Publikumseinlagen entgegen zu nehmen (Urteil des Bundesgerichts 2A.712/2006 vom 29. Juni 2007, E. 1.2). Es musste ihm somit bewusst sein, dass die Tätigkeit der B. AG und der C. AG rechtlichen Anforderungen, insbesondere einer Bewilligungspflicht, unterliegen könnte.

4.8.3.5 Ein Schuldausschlussgrund gemäss Art. 21 StGB liegt nach dem Gesagten nicht vor.

TPF 2016 28

6. Extrait du jugement de la Cour des affaires pénales dans la cause Ministère public de la Confédération et les parties plaignantes contre A. du 27 novembre 2015 (SK.2014.46)

Maxime d'accusation. Exploitation d'un moyen de preuve. Soustraction de données. Service de renseignements économiques.

Art. 9 al. 1, 141 al. 2, 325 al. 1 CPP, art. 143, 162, 273 CP, art. 47 LB

Examen de l'acte d'accusation pour les infractions de service de renseignements économiques, violation du secret d'affaires et violation du secret bancaire (consid. 1.4).

Exploitation de copies de données niée dans le cas concret dès lors que leur parfaite correspondance avec les données originales n'a pas pu être garantie (consid. 1.7).

Examen de l'élément constitutif de la «protection spéciale contre tout accès indu» au sens de l'art. 143 CP (consid. 2.1).

Appréciation dans le cas concret du chef d'accusation de service de renseignements économiques (consid. 3.4 et 3.9-3.12).

Anklageprinzip. Beweisverwertbarkeit. Unbefugte Datenbeschaffung. Wirtschaftlicher Nachrichtendienst.

Art. 9 Abs. 1, 141 Abs. 2, 325 Abs. 1 StPO, Art. 143, 162, 273 StGB, Art. 47 BankG

Prüfung der Anklageschrift bei Vorwürfen des wirtschaftlichen Nachrichtendienstes, der Verletzung des Geschäftsgeheimnisses und der Verletzung des Bankgeheimnisses (E. 1.4).

Verwertbarkeit von Datenkopien verneint, da in casu nicht sichergestellt werden konnte, dass sie mit den Originaldaten vollständig übereinstimmen (E. 1.7).

Zum Tatbestandsmerkmal der «besonderen Sicherung vor unbefugtem Zugriff» im Sinne von Art. 143 StGB (E. 2.1).

Beurteilung der Vorwürfe des wirtschaftlichen Nachrichtendienstes in concreto (E. 3.4 und 3.9-3.12).

Principio accusatorio. Utilizzabilità di una prova. Acquisizione illecita di dati. Spionaggio economico.

Art. 9 cpv. 1, 141 cpv. 2, 325 cpv. 1 CPP, art. 143, 162, 273 CP, 47 LBCR

Esame dell'accusa nel caso di imputazioni di spionaggio economico, violazione del segreto commerciale e del segreto bancario (consid. 1.4).

L'utilizzabilità di copie di dati è stata concretamente negata perché non vi è la certezza che corrispondano integralmente agli originali (consid. 1.7).

Nozione di «speciale protezione contro un accesso non autorizzato» ai sensi dell'art. 143 CP (consid. 2.1).

Valutazione concreta dell'imputazione di spionaggio economico (consid. 3.4 e 3.9-3.12).

Résumé des faits:

A., employé au service informatique de la banque suisse Z. SA, était accusé d'avoir soustrait un très grand nombre de données bancaires de son employeur enregistrées sur supports électroniques, puis, après avoir tenté d'en négocier la vente auprès de plusieurs entreprises privées étrangères, de les avoir rendues accessibles à divers organismes officiels étrangers.

La Cour des affaires pénales a reconnu A. coupable de tentative de service de renseignements économiques aggravé pour avoir proposé les données bancaires en sa possession à divers organismes publics et privés étrangers. En outre, la Cour a acquitté A. de certains autres reproches de service de renseignements économiques, du reproche de soustraction de données, ainsi que des reproches de violation du secret commercial et violation du secret bancaire, lorsqu'elle n'a pas classé la procédure, en raison de la prescription de l'action pénale.

Extraits des considérants:

1.4 Maxime d'accusation

1.4.1 Aux termes de l'art. 9 al. 1 CPP, une infraction ne peut faire l'objet d'un jugement que si le ministère public a déposé auprès du tribunal compétent un acte d'accusation dirigé contre une personne déterminée sur la base de faits précisément décrits. La maxime d'accusation ancrée dans cette disposition est un principe fondamental de l'Etat de droit, qui implique notamment que le juge est lié par l'ampleur de l'acte d'accusation et ne peut juger que les comportements (actions ou omissions) reprochés à l'accusé qui y sont décrits d'une manière précise. En ce sens, la maxime d'accusation limite l'objet de la procédure; le juge n'a ni le devoir ni la compétence de dépasser les bornes établies par l'acte d'accusation (SCHUBARTH, Commentaire romand, Bâle 2011, n° 1 à 4 ad art. 9 CPP).

L'art. 325 al. 1 let. f CPP impose au ministère public de désigner dans l'acte d'accusation, le plus brièvement possible, mais avec précision, les actes reprochés au prévenu, le lieu, la date et l'heure de leur commission ainsi que leurs conséquences et le mode de procéder de l'auteur.

1.4.2 En l'espèce, il appert, à la lecture de l'acte d'accusation, que le dernier fait daté et clairement décrit de service de renseignements économiques reproché à A. aurait eu lieu le 3 juillet 2008. Il s'agit de la transmission d'un courriel contenant une annexe cryptée au dénommé B. Après cette date, les seuls reproches formulés à l'encontre de A. sont d'avoir «continué à communiquer» avec cette personne et de l'avoir rencontrée en décembre et janvier 2009, sans qu'aucun acte précis susceptible de tomber sous le coup de l'art. 273 CP ne soit formulé. Les autres actes reprochés, toujours au chef de l'art. 273 CP, qui seraient, pour partie, postérieurs au 3 juillet 2008, consistent en le fait d'avoir proposé les fichiers en sa possession, «de mars 2008 à ce jour, dans différents pays qui ressortent d'écrits de l'accusé ou d'interviews dans les médias et/ou qui se sont manifestés ensuite en Suisse par des demandes d'entraide administratives ou judiciaires». Les pays en question seraient (outre la France, l'Allemagne et le Royaume-Uni) l'Espagne, l'Inde, la Grèce, l'Italie et la Belgique. Là encore, aucun acte ponctuel, ni daté, ni décrit, susceptible d'être individualisé et examiné n'est précisément reproché au prévenu. Le dossier ne permet pas d'établir l'existence et le contenu d'éventuels entretiens postérieurs au 3 juillet 2008 entre A. et un agent officiel étranger. Il n'est en outre pas établi que A. ait, à un quelconque moment, assisté un service étranger dans l'examen de

données de la banque Z. SA. Le dossier n'apporte pas la preuve que A. ait eu des contacts avec des services étatiques étrangers espagnols, indiens, grecs, italiens ou belges, entre mars 2008 et le 2 décembre 2014.

Ni dans l'acte d'accusation, ni dans le dossier d'ailleurs, ne figure la moindre indication quant aux modalités des prétendus actes perpétrés non seulement après le 3 juillet 2008, en faveur de quelque Etat que ce soit, mais également, depuis mars 2008, en faveur de l'Italie, de l'Espagne, de la Grèce, de l'Inde ou de la Belgique (indication de temps et de lieu, *modus operandi* de l'auteur, etc.). Une telle description d'un crime ne satisfait manifestement pas à l'exigence de précision découlant des art. 9 et 325 al. 1 let. f CPP. En vertu de la maxime d'accusation, la Cour est liée par l'absence d'allégation précise des infractions de service de renseignements économiques qui auraient été perpétrées par le prévenu après le 3 juillet 2008 et, d'une manière générale, en faveur des autres destinataires précités, que sont l'Italie, l'Espagne, la Grèce, l'Inde, la Belgique, ou de leurs agents, de sorte que le prévenu est acquitté des reproches du chef de l'art. 273 CP y relatifs.

Au surplus, le Ministère public de la Confédération (MPC) s'appuie uniquement sur un résumé, fait par un membre de l'Ambassade suisse présent dans le public, des réponses données en audience par le prévenu au Ministère public espagnol, lors de la procédure d'extradition à la Suisse en avril 2013, pour alléguer que c'est A. qui aurait donné accès aux informations aux autorités italiennes et espagnoles. Concernant les autres pays, le MPC se réfère à plusieurs demandes d'entraide administrative ou judiciaire que ces nations ont adressées à la Suisse, en relation avec des personnes ou des sociétés dont les noms figuraient dans les données en possession du prévenu. Toutefois, rien n'indique que le prévenu serait à l'origine de leur transmission. En revanche, le procureur de la République française a informé le MPC qu'il avait, en exécution de demandes d'entraide judiciaire internationale, transmis au Parquet de Turin et à celui de Würzburg les données relatives aux ressortissants italiens, respectivement allemands, récoltées suite à la perquisition du 20 janvier 2009 à Castellar. Il est en outre établi que les autorités fiscales françaises ont transmis à leurs homologues italiens les informations ayant servi de base aux redressements fiscaux de clients de la banque Z. SA résidant en Italie.

1.4.3 Pour décrire les actes reprochés aux chefs des art. 162 CP et 47 LB, l'acte d'accusation renvoie au chiffre énonçant les activités reprochées d'infraction à l'art. 273 CP. Dès lors, ce qui a été dit en matière de principe

accusatoire pour les infractions à l'art. 273 CP vaut également en ce qui concerne les infractions de violations du secret commercial et du secret bancaire (v. *supra* consid. 1.4.2). En vertu de la maxime d'accusation, la Cour est liée par l'absence d'allégation précise pour les infractions aux art. 162 CP et 47 LB qui auraient été perpétrées après le 27 novembre 2008 (puisqu'avant cette date, l'action pénale pour ces infractions est prescrite). Le prévenu est partant acquitté des reproches du chef des art. 162 CP et 47 LB postérieurs à cette date.

1.7 Exploitabilité des supports de données transmis par les autorités françaises

1.7.1 A teneur de l'art. 139 al. 1 CPP, les autorités pénales mettent en œuvre tous les moyens de preuves licites qui, selon l'état des connaissances scientifiques et l'expérience, sont propres à établir la vérité. En application de l'art. 141 al. 2 CPP, les preuves qui ont été administrées d'une manière illicite ou en violation des règles de validité par les autorités pénales ne sont pas exploitables, à moins que leur exploitation soit indispensable pour élucider des infractions graves.

Suite au départ de A. du territoire suisse pour, selon les informations recueillies, le sud de la France, le MPC a requis des autorités compétentes françaises, par commission rogatoire du 9 janvier 2009, outre la localisation, l'interpellation et l'audition du prévenu, la perquisition de son lieu de résidence et la saisie de tous les documents et pièces utiles à l'enquête. En date du 20 janvier 2009, les autorités françaises, accompagnées de représentants des autorités de poursuite suisses, ont effectué une perquisition en France, à l'endroit où le prévenu avait été localisé. À cette occasion, deux ordinateurs, de marques QBIC et Apple, ont notamment été saisis.

Ce n'est qu'en date du 26 janvier 2010 que, toujours dans le cadre de l'entraide judiciaire, les autorités françaises ont transmis aux autorités suisses un rapport de l'Institut de Recherches criminelles de la Gendarmerie Nationale (IRCGN), huit DVD-Rom annexés audit rapport, contenant des extraits du contenu des disques durs des deux ordinateurs QBIC et Apple, ainsi notamment que deux clones des disques durs des ordinateurs saisis au lieu de résidence français du prévenu en janvier 2009. Les supports de données originaux n'ont, quant à eux, pas été remis aux autorités suisses.

1.7.2 Le procédé de copie forensique avec empreinte numérique, utilisé par les spécialistes de la Police judiciaire fédérale (PJF) pour créer une copie des supports de données saisis au domicile du prévenu à Genève, permet d'attester l'intégrité des données et de garantir qu'aucune opération d'écriture ne peut être effectuée durant le processus de création de la copie (support cible) à partir du support de données source. À l'inverse, le processus de copie utilisé par les autorités françaises ne permet pas de garantir que le contenu du support cible (clone) corresponde en tous points au contenu du support original.

À cela s'ajoute que l'instruction a, en l'occurrence, fourni des indices que les copies remises par les autorités françaises ne correspondaient pas aux originaux trouvés le 20 janvier 2009 au lieu de résidence français du prévenu. Premièrement, l'analyse effectuée par les experts de la PJF a révélé des divergences entre le contenu des disques clones et celui des DVD remis par les autorités françaises, alors que les deux types de supports étaient censés contenir les mêmes données, soit celles enregistrées sur les disques durs des ordinateurs saisis au lieu de résidence français du prévenu. Deuxièmement, pour certains fichiers remis par les autorités françaises, la dernière date de modification était ultérieure à la date de la perquisition au lieu de résidence français du prévenu.

Dans ces conditions, la Cour ne saurait retenir que l'un ou l'autre des deux types de supports remis par les autorités françaises (DVD ou clones) contenait les données intègres des disques durs originaux des ordinateurs saisis en France.

Vu l'ensemble de ces éléments, les données transmises par les autorités françaises par le biais de l'entraide judiciaire internationale ne sont pas exploitables.

2.1 A teneur de l'art. 143 CP, commet une infraction celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura soustrait, pour lui-même ou pour un tiers, des données enregistrées ou transmises électroniquement ou selon un mode similaire, qui ne lui étaient pas destinées et qui étaient spécialement protégées contre tout accès indu de sa part.

Cet article protège le droit du bénéficiaire légitime de disposer de ses données et de ses logiciels. Le fait que les données aient un caractère confidentiel ne joue aucun rôle (Message du 24 avril 1991 concernant la

modification du CP suisse et du CP militaire, FF 1991 II p. 978). D'autres dispositions pénales existent en effet pour assurer cette protection, notamment les art. 162 CP et 47 LB.

Le Message du Conseil fédéral différencie les données publiques des données protégées, pour expliquer que le législateur a voulu restreindre le champ d'application de la norme. Le critère de la protection des données a été voulu pour limiter la protection pénale à certaines données. À défaut, toute soustraction de données appartenant à autrui tomberait sous le coup de cette disposition, ce qui constituerait une extension excessive de la protection (ex: école, université, bibliothèque; ces institutions mettent à disposition des ordinateurs, donnant accès à leurs données, pour travailler, étudier, etc.; FF 1991 II p. 978). Dans son Message du 18 juin 2010 relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité, le Conseil fédéral a rappelé la volonté du législateur relative à l'exigence de la protection spéciale du système informatique, qui est de limiter le champ d'application de l'art. 143 CP aux cas dans lesquels la personne ayant légalement accès aux données manifeste sa volonté d'empêcher que des tiers n'accèdent à ses données ou de restreindre cet accès. Mis à part le verrouillage de locaux et d'armoires, par exemple, l'utilisation d'un chiffrement, de codes d'accès, de clefs biométriques ou de mots de passe est également une manifestation de cette intention. La protection doit être *habituellement suffisante* pour empêcher un accès illégal. Il n'est pas nécessaire, par exemple, que des mesures de protection spécifiques, allant au-delà d'une protection habituelle sur le marché contre les virus et les accès illicites, aient été prises. La norme pénale ne s'applique pas, par contre, à une attaque contre des données non protégées ou à leur utilisation illicite (FF 2010 p. 4283).

L'art. 143 CP ne vise ainsi pas à protéger les données de manière globale, mais seulement les données que le propriétaire ne veut pas laisser accessibles à l'auteur. Ce dernier ne doit pas être légitimé à disposer des données et il doit pouvoir reconnaître clairement que le titulaire des données ne veut pas qu'il y accède. Il n'y a pas de mesures suffisantes dans le cas d'un employé qui ne rencontre aucune mesure de sécurité spécifique lui entravant l'accès aux données détenues par son employeur, si ce n'est une barrière morale (TC VS RVJ 2006, 222; WEISSENBERGER, Basler Kommentar, 3e éd., Bâle 2013, n° 18 ad art. 143 CP). Il n'est en revanche pas exigé que le propriétaire possède de meilleures compétences informatiques que l'auteur, ni que la protection ait une efficacité particulière. L'auteur doit en tous cas pouvoir reconnaître que les données

sont protégées (MÉTILLE/ AESCHLIMANN, Infrastructures et données informatiques: quelle protection au regard du code pénal suisse?, RPS 132/2014, p. 283 ss, 291 et auteurs cités, not. CORBOZ, STRATENWERTH/JENNY/BOMMER). L'accès doit être interdit aux personnes non autorisées au moyen de mesures techniques (MÜLLER, La cybercriminalité économique au sens étroit – Analyse approfondie du droit suisse et aperçu de quelques droits étrangers, thèse, Genève/ Zurich/Bâle 2012, p. 32); une interdiction morale ou contractuelle ne suffit pas, pour celui à qui l'accès aux données est permis, selon la doctrine (DUPUIS ET AL., Petit commentaire, Bâle 2012, n° 14 ad art. 143 CP). L'auteur doit franchir des obstacles dont il ne peut ignorer le sens pour se procurer ces données (FF 1991 II p. 979). Les obstacles doivent être matériels et non moraux, légaux ou contractuels. Les instructions, les interdictions orales ou écrites, ou encore les mesures d'organisation visant à séparer les fonctions au sein du personnel ne constituent pas des mesures de sécurité suffisantes au sens de l'art. 143 CP (SCHMID, Computer- sowie Check- und Kreditkarten-Kriminalität, Zurich 1994, n° 39 ad art. 143 CP; MÉTILLE/AESCHLIMANN, op. cit., p. 291). Les standards de protection requis sont plus élevés, s'agissant des données sensibles de la vie économique, telles celles relatives aux clients d'une banque, du fait que l'ayant droit doit prendre en compte de potentiels auteurs professionnels (WEISSENBERGER, op. cit., n° 19 ad art. 143 CP).

Il s'agit, pour l'auteur, de se procurer des données prélevées sans droit, soit sans autorisation, sur un support de données ou un système de traitement des données qui ne lui sont pas destinées et de les exploiter à son profit (FF 1991 II p. 948, 977). S'il est habilité à disposer des données mais qu'il outrepasse les limites de son droit d'utilisation (posées par la loi, le contrat ou la morale), l'art. 143 CP ne s'applique pas. L'abus de confiance portant sur des données informatiques ne tombe donc pas sous le coup de cette disposition (FF 1991 II p. 978). Un projet d'alinéa 3 à l'art. 143 CP, qui aurait sanctionné ce type d'abus de confiance, avait été proposé aux Chambres fédérales en 2010, avant d'être classé en 2012 par le Conseil des Etats (initiative parlementaire n° 10.456; BO 2012 S 540; v. ég. l'initiative parlementaire n° 10.451 retirée dans la foulée au Conseil National). Le libellé dudit alinéa était le suivant: «celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement, s'approprie des données auxquelles il a accès dans le cadre de ses tâches ou utilise de manière illégitime de telles données à son profit ou au profit d'un tiers est puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire» (v.

ég. PERRIN, La protection pénale des données informatiques de l'entreprise, ECS 8/11 605, p. 608).

3.4 Au moment des faits, soit entre février et juillet 2008, A. était effectivement en possession d'informations personnelles et financières détaillées concernant plus de 120'000 clients et anciens clients de la banque Z. SA, représentant un volume d'environ 70 gigas, comme annoncé dans ses lettres à C. et à D. en avril 2008. Selon E., en novembre 2006, A. lui aurait dit qu'il possédait une base de données qu'il souhaitait monnayer. Dès mars 2007 en tout cas, le prévenu travaillait à récolter ou à regrouper de telles données à des fins privées. Des échanges de courriels avec le dénommé L., en juin 2007, il apparaît en outre que A. détenait, à ce moment-là, pour le Moyen-Orient, les données bancaires de 11'966 clients répartis sur 12 pays. Le nombre de 120'000 clients ressort également d'un courriel envoyé par E. à un banquier libanais en janvier 2008. Le volume et la nature des informations bancaires en possession du prévenu ressortent enfin des données retrouvées sur des supports informatiques privés au jour de la perquisition du domicile de A. à Genève en décembre 2008. A. n'a jamais disposé d'autres données bancaires que celles de son employeur de l'époque. Seules des données provenant de la banque Z. SA ont été retrouvées dans le matériel informatique saisi au domicile et au lieu de travail du prévenu le 22 décembre 2008. Il s'agit de données structurelles, réglementaires, mais surtout de très nombreuses données personnelles et financières de clients et de comptes provenant de la banque Z. SA. En ce qui concerne les supports de données trouvés lors de la perquisition du domicile de la famille A. à Genève, rien au dossier ne permet de penser qu'un tiers, soit une autre personne que le prévenu ou, pour l'ordinateur Apple PowerBook, son épouse, les aurait utilisés.

À l'époque des faits, l'entité visée, à savoir la banque Z. SA, était une grande banque privée ayant son siège en Suisse (total du bilan 2008: Fr. 73'314'354'000, [Banque nationale suisse, Les banques suisses, Zurich 2009, B15]). De jurisprudence constante, les listes de clients des grandes entreprises installées en Suisse et les informations portant sur les relations bancaires sont protégées par l'art. 273 CP. Les données bancaires (tant celles personnelles et financières des clients que celles internes à la banque, ayant trait à son organisation, à sa structure et à son système de gestion des relations bancaires) constituent des secrets au sens de cette disposition (v. arrêts du Tribunal pénal fédéral SK.2014.32 du 19 décembre 2014; SK.2013.37 du 10 décembre 2013, consid. 3.1.2; SK.2011.21 du 15 décembre 2011).

3.9 Au moment de son départ au Liban, en février 2008, A. détenait, sur divers supports informatiques privés, une somme considérable d'informations issues des banques de données de la banque Z. SA. Il avait créé ou fait créer un site internet, une messagerie électronique, une présentation Powerpoint au nom de la société MM., des cartes de visite au faux nom de Ruben G. *Sales Manager* de cette société. Il avait également planifié le voyage au Liban, soit réservé des billets d'avion et fait prendre contact avec plusieurs employés de banque. En procédant, entre le 4 et le 8 février 2008, aux présentations du produit qu'il souhaitait vendre aux agents de cinq banques libanaises (banque 3., banque 4., banque 5., banque 6. à Beyrouth et banque d'investissement 7.), il a extériorisé sa volonté de rendre accessibles les données en sa possession et ainsi franchi le pas décisif menant à la commission de cinq infractions de service de renseignements économiques.

Suite à l'échec de ses tentatives au Liban, même après les courriels de relance à O. et Q., A. a proposé les mêmes informations, par courriels à quatre organismes officiels étrangers (*Bundesnachrichtendienst* allemand, *Secretary of State for Foreign and Commonwealth Affairs* [*SOSFA*] et *Her Majesty's Revenue and Customs* [*HMRC*] britanniques et la Division nationale d'investigations financières [DNIF] française). Les courriers électroniques envoyés aux organismes officiels étrangers constituent autant de manifestations claires de la volonté de A. de rendre accessibles les secrets d'affaires en sa possession.

Dans chacun des cas, la réalisation d'un seul élément constitutif objectif faisait encore défaut. Toutefois, au vu notamment de ses motivations et du *modus operandi* adopté, il ne fait aucun doute que A., sur le principe, était déjà fermement résolu à donner accès aux données de la banque Z. SA aux organismes officiels et privés étrangers avec lesquels il cherchait à entrer en négociations. Le mode opératoire du prévenu, notamment les messages d'accroche utilisés afin d'entrer en négociations (plutôt que l'envoi immédiat des données), les destinataires choisis et l'usage d'une fausse identité dans le cadre de ces négociations, démontre que A. entendait obtenir une contreprestation en échange des données en sa possession.

Par ses actes, A. a commencé l'exécution de neuf infractions réprimées à l'art. 273 al. 2 CP. Il s'agit d'autant de tentatives de service de renseignements économiques (art. 22 al. 1 CP).

3.10 Les seuls secrets d'affaires que A. a effectivement rendus accessibles à un organisme étranger, au sens de l'art. 273 al. 2 CP, consistent en ceux transmis par courriel du 3 juillet 2008 à un agent étatique français. Il s'agit du second reproche du MPC à l'encontre du prévenu. Cet acte, qui réalise l'ensemble des conditions de l'infraction à l'art. 273 al. 2 CP, constitue une infraction consommée de service de renseignements économiques.

3.11. Au moment des faits, la banque Z. SA était une grande banque privée implantée en Suisse (v. *supra* consid. 3.4). La place financière suisse était, comme elle l'est encore aujourd'hui, importante tant pour l'économie nationale que pour l'image de la Confédération à l'étranger.

3.11.1 Les tentatives de service de renseignements économiques commises par A. ont partant mis en danger l'indépendance de la Suisse, son économie et touché la place financière suisse et ses relations avec d'autres Etats. Vu la nature et le volume des informations en cause, chacune des tentatives perpétrées par A. constitue un acte de service de renseignements économiques aggravé, au sens de l'art. 273 al. 3 CP.

Dans ces conditions, A. doit être déclaré coupable de tentatives de service de renseignements économiques aggravé, au sens de l'art. 273 al. 2 et 3 CP, pour avoir, entre le 4 et le 8 février 2008, présenté aux représentants des banques 3., 4., 5., 6. à Beyrouth et de la banque d'investissement 7. un produit qu'il souhaitait vendre, consistant en une base de données contenant des informations personnelles et financières sur des clients de la banque Z. SA, ainsi que pour avoir proposé une telle base de données au *Bundesnachrichtendienst* allemand le 7 mars 2008, à deux organismes officiels du Royaume-Uni (SOSFA et HMRC) le 19 mars 2008, ainsi qu'à un organisme officiel français (DNIF) le 2 avril 2008.

3.11.2 Quant au fichier transmis à l'agent B. le 3 juillet 2008, il contenait des données personnelles et bancaires concernant sept personnes (physiques ou morales). Dès lors, quand bien même ces données étaient celles d'une grande banque Suisse, leur volume n'était pas objectivement susceptible de mettre en danger la place financière et économique suisse, ni même ses relations avec d'autres Etats. Partant, cette transmission ne constitue pas un cas grave, au sens de l'art. 273 al. 3 CP, de sorte que l'action pénale y relative est prescrite.

3.12 Concernant enfin la présentation faite au bureau de représentation de la banque 1. (SUISSE) SA au Liban, la condition objective du destinataire

étranger fait défaut. Les autres conditions objectives et subjective de l'infraction étant réalisées, il s'agit de déterminer si cet acte constitue une tentative de service de renseignements impossible, punissable en application des art. 273 al. 2 et 22 al. 1 *in fine* CP.

Dans un arrêt récent, le Tribunal fédéral semble exclure que les délits de mise en danger abstraite puissent être qualifiés de délits impossibles et punis. En effet, les délits impossibles ne doivent être punissables que dans la mesure où ils représentent une mise en danger réelle de l'ordre juridique. Outre la volonté de commettre une infraction, il doit exister une mise en danger objective minimale due au comportement de l'auteur; un délit impossible objectivement sans danger – comme une tentative ridicule – ne met pas en danger l'ordre juridique, de sorte que son auteur, même s'il n'a pas agi en faisant preuve d'un grave défaut d'intelligence, doit demeurer impuni (ATF 140 IV 150 consid. 3.6 – JdT 2015 IV 114). Dans l'arrêt du Tribunal pénal fédéral SK.2013.37 du 10 décembre 2013 précité, l'auteur a été condamné pour tentative de service de renseignements économiques, pour s'être adressé à l'avocat suisse d'une entreprise russe, afin de vendre à cette dernière des données secrètes. Même s'il ne s'est pas adressé directement à un agent étranger, son but était de mettre à disposition de l'entreprise russe les données en question en contrepartie de l'argent que l'entreprise lui verserait. L'avocat n'était qu'un intermédiaire pour atteindre le but (sans pour autant être un agent de l'organisme étranger, au sens de l'art. 273 CP), intermédiaire par ailleurs également susceptible de tomber sous le coup de l'art. 273 al. 2 CP s'il transmettait les données en question à son client étranger. Le délit de mise en danger abstraite n'a, dans ce cas, pas été considéré comme impossible et a été réprimé.

En l'espèce, le prévenu s'est adressé à un représentant suisse d'une banque suisse, sur territoire étranger. Même si sa volonté était, depuis le 17 juin 2007 en tout cas, celle de vendre des données de la banque Z. SA à un organisme étranger, en agissant de la sorte, il n'a aucunement mis en danger l'économie ni la souveraineté de la Suisse. Partant, le prévenu est acquitté de ce reproche.