Bundesstrafgericht
Tribunal pénal fédéral
Tribunale penale federale
Tribunal penal federal

Numéro de dossier: BB.2019.248-249

Décision du 26 janvier 2021
Cour des plaintes

Composition	Les juges pénaux fédéraux Roy Garré, président, Cornelia Cova et Patrick Robert-Nicoud, la greffière Daphné Roulin
Parties	**1. A.,** **2. B. SA,** tous deux représentés par Me Myriam Fehr-Alaoui, avocate, Me Jean-François Ducrest, avocat, Me Paolo Bernasconi, avocat, ainsi que par Me Daniel Zappelli, avocat, recourants **contre** **MINISTÈRE PUBLIC DE LA CONFÉDÉRATION**, intimé
Objet	Extension de l'instruction (art. 311 al. 2 CPP); admission de la partie plaignante (art. 118 ss en lien avec l'art. 104 al. 1 let. b CPP)

Faits:

A. Le 11 décembre 2017, le « groupe Bb. » et A. administrateur président avec signature individuelle de B. SA ont déposé, par l'entremise de Me Ducrest, une « dénonciation formelle (art. 301 al. 1 CPP) » auprès du Ministère public de la Confédération (ci-après: MPC) à l'encontre de D. pour les infractions, à tout le moins, de soustraction de données (art. 143 CP), accès indu à un système informatique (art. 143bis CP), services de renseignements économiques (art. 273 CP) et violation du secret de fabrication ou de secret commercial (art. 162 CP; act. 1.4).

B. Suite à cette dénonciation, le MPC mène depuis le 19 novembre 2018 une instruction pénale contre D. pour service de renseignements économiques au sens de l'art. 273 CP, procédure référencée sous le n. SV.18.0492 (cf. act. 1.23).

C. Par lettres des 14 février, 19 mars et 16 mai 2019, A. et B. SA ont requis l'extension de l'instruction à l'infraction de soustraction de données (art. 143 CP), en se référant à leur « dénonciation » du 11 décembre 2017, et se sont constitués en qualité de parties plaignantes (act. 1.24 à 1.26).

Le 12 juin 2019, le MPC n'a pas étendu la procédure et a estimé que les intéressés ne pouvaient pas revêtir la qualité de partie plaignante dans le cadre de la procédure ouverte (act. 1.27).

A. et B. SA ont demandé au MPC de revoir sa position (lettres des 18 juin, 24 juillet et 4 octobre 2019: act. 1.28 à 1.30).

Par acte du 11 novembre 2019 (*recte*: octobre), avec indication de la voie de recours, le MPC a maintenu sa position (act. 1.1).

D. Le 24 octobre 2019, A. et B. SA – représentés par Me Ducrest et Me Fehr-Alaoui – forment un recours contre l'acte précité auprès de la Cour des plaintes du Tribunal pénal fédéral (act. 1). Ils concluent, sous suite de frais et dépens, principalement, à l'annulation de la décision litigieuse, à ce que l'instruction pénale contre D. du chef de soustraction de données (art. 143 CP) soit ouverte, respectivement étendue, au renvoi de la cause au MPC pour instruction en ce sens, à leur admission en qualité de partie plaignante dans la procédure ainsi que celle étendue et de réserver leur droit de solliciter la répétition des actes d'instruction. A titre subsidiaire, ils prennent les mêmes conclusions à la différence que, à la place de conclure directement à l'ouverture de l'instruction, ils concluent à ce que la cause soit

renvoyée au MPC pour qu'il ouvre, respectivement étende, l'instruction pénale contre D. du chef de soustraction de données (art. 143 CP).

E. Dans le cadre de l'échange d'écritures, le MPC conclut au rejet du recours (act. 4 et 15). Aux termes de leur réplique du 9 décembre 2019, les recourants persistent intégralement dans les conclusions prises en tête de leur mémoire de recours (act. 13). Le 19 décembre 2019, ils se déterminent spontanément sur la duplique du MPC (act. 17).

F. Par lettre spontanée du 12 mai 2020 (act. 19), A. et B. SA transmettent à la Cour un acte du 30 avril 2020 rendu par le MPC dans le cadre d'une autre procédure pénale référencée sous le n. SV.17.1802 (instruction pénale ouverte le 8 décembre 2017 contre A. et E.) En substance, dans cet acte, la Procureure fédérale en charge de la cause communiquait sa décision d'exploiter les données extraites du serveur de B. SA ainsi que toutes les preuves dérivées de celles-ci (act. 19.1).

Invité à se déterminer, le MPC indique que ce document n'influence pas le sort du présent recours et maintient que celui-ci doit être rejeté (observations du 20 mai 2020: act. 21).

Les 5 et 12 juin 2020, les recourants font part de leurs déterminations spontanées (act. 24 et 26). Le 6 juillet 2020, Me Fehr-Alaoui signifie à la Cour de céans qu'ils sont désormais quatre avocats conjointement coconstitués avec élection de domicile en son étude (act. 28).

Les arguments et moyens de preuve invoqués par les parties seront repris, si nécessaire, dans les considérants en droit.

La Cour considère en droit:

1.

1.1 La Cour des plaintes du Tribunal pénal fédéral examine d'office la recevabilité des recours qui lui sont adressés (v. GUIDON, Die Beschwerde gemäss Schweizerischer Strafprozessordnung, 2011, n. 546 et les références citées).

1.2 Les décisions du MPC peuvent en principe faire l'objet d'un recours devant la Cour des plaintes du Tribunal pénal fédéral (art. 393 al. 1 let. a CPP et art. 37 al. 1 de la loi fédérale du 19 mars 2010 sur l'organisation des autorités pénales de la Confédération [LOAP; RS 173.71]). Le refus du MPC d'étendre

l'instruction de la procédure à une autre infraction s'apparente à une décision de non-entrée en matière (arrêt du Tribunal fédéral 6B_1276/2019 du 27 février 2020 consid. 3.1 et la référence citée; v. décision du Tribunal pénal fédéral BB.2016.376-384 du 2 février 2018 consid. 2.4.5 et la référence citée: dans ces cas, il s'agit d'un refus du ministère public d'étendre l'instruction à d'autres prévenus), laquelle peut faire l'objet d'un recours devant la Cour de céans (art. 322 al. 2 CPP par renvoi de l'art. 310 al. 2 CPP, cf. art. 309 al. 1 CPP). Conformément à l'art. 393 al. 2 CPP, le recours peut être formé pour violation du droit, y compris l'excès et l'abus du pouvoir d'appréciation, le déni de justice et le retard injustifié (let. a), la constatation incomplète ou erronée des faits (let. b) ou l'inopportunité (let. c).

1.3 Interjeté le 24 octobre 2019, le recours a été déposé dans le délai de dix jours dès la notification de la décision attaquée (cf. art. 384 et 396 al. 1 CPP), soit le 14 octobre 2019, et a été ainsi formé en temps utile.

2. Le recours contient deux volets, à savoir, d'une part, l'extension de l'instruction de la procédure ouverte par le MPC à l'infraction de soustraction de données (art. 143 CP) et, d'autre part, leur admission en qualité de partie plaignante dans le cadre de la procédure pénale ouverte (et étendue) contre D. Il y a lieu de traiter ces deux aspects distinctement et d'examiner à chaque fois la question de la recevabilité, en particulier en ce qu'il concerne la qualité pour recourir.

Extension de l'instruction

3. Il convient d'examiner la qualité pour recourir des recourants relative à leur requête d'extension de l'instruction à l'infraction de soustraction de données (art. 143 CP).

3.1 La qualité pour recourir de la partie plaignante (art. 118 al. 1 CPP; *partie* à la procédure au sens de l'art. 104 al. 1 let. b CPP) contre une ordonnance de classement, de non-entrée en matière ou de refus d'étendre l'instruction est subordonnée à deux conditions cumulatives: ses droits doivent être directement touchés par l'infraction (cf. art. 115 al. 1 CPP) et elle doit faire valoir un intérêt juridiquement protégé à l'annulation de la décision (cf. art. 382 al. 1 CPP). En règle générale, seul peut se prévaloir d'une atteinte directe le titulaire du bien juridique protégé par la disposition pénale qui a été enfreinte (ATF 141 IV 1 consid. 3.1 p. 5; 129 IV 95 consid. 3.1 et les arrêts cités). Par ailleurs, l'intérêt doit être actuel et pratique (arrêt du Tribunal fédéral 1B_157/2019 du 9 juillet 2019 consid. 2).

3.2 En l'espèce, les recourants concluent à une extension de l'instruction à

l'infraction de soustraction de données au sens de l'art. 143 CP. Cette disposition vise la protection du droit du bénéficiaire légitime de disposer de ses données et de ses logiciels (TPF 2016 28 consid. 2.1). Cette infraction a ainsi pour but de protéger les intérêts privés. Les recourants se prévalent de la soustraction par D., ex-employé de B. SA, de 90 gigaoctets de données informatiques du groupe Bb. et du contenu de la boîte e-mails de A. et E. En tant titulaire des données informatiques, B. SA est directement touchée et revêt ainsi la qualité de lésé (cf. art. 115 al. 1 CPP). Par une déclaration expresse, elle peut se constituer partie plaignante (cf. art. 118 al. 1 CPP). Quant à A., il allègue également être le propriétaire, respectivement le titulaire, de ces données soustraites (act. 1 n. 73). La question pourra souffrir de demeurer ouverte de savoir si A. est le bénéficiaire légitime de disposer de ces données, respectivement s'il est directement touché et donc lésé. En effet, au vu des motifs développés ci-après, le recours doit de toute manière être rejeté.

3.3 Le MPC fait valoir que les recourants ont renoncé définitivement à leurs droits de parties plaignantes en raison du dépôt d'une « dénonciation formelle (art. 301 al. 1 CPP) », et non d'une plainte pénale, de sorte qu'ils n'ont pas un intérêt juridiquement protégé à l'annulation de la décision (art. 382 al. 1 CPP). D'après le MPC, la dénonciation de A. et B. SA a valeur de renonciation définitive au sens de l'art. 120 al. 1 CPP. La Cour de céans constate en l'occurrence qu'en déposant une dénonciation et non pas une plainte pénale, il est clair que les recourants ne se sont pas constitués parties plaignantes, alors qu'ils seraient lésés eu égard notamment à la violation alléguée de l'art. 143 CP (cf. *supra*). Il ne ressort néanmoins pas des termes de leur dénonciation qu'ils ont expressément renoncé d'user de leurs droits au sens de l'art. 120 al. 1 CP. Une renonciation à user de ses droits en tant que partie plaignante doit être faite sans équivoque (« *unmissverständlich* »), dès lors qu'elle est définitive (arrêts du Tribunal fédéral 1B_446/2018 du 14 novembre 2018 consid. 4.4; 1B_188/2015 du 9 février 2016 consid. 5.5). *In casu*, en l'absence de renonciation expresse, la Cour considère que les recourants n'avaient pas renoncé à leur qualité de partie plaignante. Ils pouvaient par conséquent encore se déclarer parties plaignantes tant que la procédure préliminaire n'était pas close (cf. art. 118 al. 3 CPP). Dit délai est en l'espèce respecté, dès lors que A. et B. SA se sont constitués parties plaignantes au civil et au pénal par lettres des 31 janvier et 14 février 2019 (act. 1.22 et 1.24). Partant, contrairement au raisonnement du MPC, les recourants ont valablement présenté leur constitution en qualité de partie plaignante.

4. Les recourants font valoir que le refus d'extension de l'instruction du MPC violerait la maxime d'instruction (art. 6 CPP), le caractère impératif de la

poursuite (art. 7 CPP) ainsi que les dispositions permettant de rendre une ordonnance de non-entrée en matière (art. 310 al. 1 let. a CPP). Dans ce contexte, le MPC aurait également violé l'art. 393 al. 2 let. b CPP en constatant de manière incomplète des faits.

4.1

4.1.1 Conformément à l'art. 311 al. 2, 1ère phrase, CPP, le ministère public peut étendre l'instruction à d'autres prévenus et à d'autres infractions, l'art. 309 al. 3 CPP étant alors applicable. L'extension de l'instruction suppose que les conditions pour l'ouverture d'une instruction (art. 309 al. 1 CPP) soient réalisées en ce qui concerne les autres faits, respectivement les autres personnes, visés (GRODECKI/CORNU, Commentaire romand, 2ème éd. 2019, n° 15 ad art. 311 CPP).

4.1.2 Si le ministère public refuse la requête d'extension, sa décision s'apparente à une non-entrée en matière au sens de l'art. 310 CPP (arrêt du Tribunal fédéral 6B_1276/2019 du 27 février 2020 consid. 3.1 et la référence citée). Conformément à l'art. 310 al. 1 let. a CPP, le ministère public rend immédiatement une ordonnance de non-entrée en matière s'il ressort de la dénonciation ou du rapport de police que les éléments constitutifs de l'infraction ou les conditions à l'ouverture de l'action pénale ne sont manifestement pas réunis. Selon la jurisprudence, cette disposition doit être appliquée conformément à l'adage « *in dubio pro duriore* ». Celui-ci découle du principe de la légalité (art. 5 al. 1 Cst. et 2 al. 1 CPP en relation avec les art. 309 al. 1, 319 al. 1 et 324 CPP; ATF 138 IV 86 consid. 4.2 p. 91) et signifie qu'en principe, un classement ou une non-entrée en matière ne peuvent être prononcés par le ministère public que lorsqu'il apparaît clairement que les faits ne sont pas punissables ou que les conditions à la poursuite pénale ne sont pas remplies. La procédure doit se poursuivre lorsqu'une condamnation apparaît plus vraisemblable qu'un acquittement ou lorsque les probabilités d'acquittement et de condamnation apparaissent équivalentes, en particulier en présence d'une infraction grave. En effet, en cas de doute s'agissant de la situation factuelle ou juridique, ce n'est pas à l'autorité d'instruction ou d'accusation mais au juge matériellement compétent qu'il appartient de se prononcer (ATF 143 IV 241 consid. 2.2.1 p. 243; 138 IV 86 consid. 4.1.2 p. 91 et les références citées; cf. récemment arrêt du Tribunal fédéral 6B_641/2020 du 8 septembre 2020 consid. 4.1).

L'établissement de l'état de fait incombe principalement au juge matériellement compétent pour se prononcer sur la culpabilité du prévenu. Le ministère public et l'autorité de recours n'ont dès lors pas, dans le cadre d'une décision de classement d'une procédure pénale, respectivement à l'encontre d'un recours contre une telle décision, à établir l'état de fait comme le ferait le juge du fond. Des constatations de fait sont admises au stade du

classement, dans le respect du principe « *in dubio pro duriore* », soit dans la mesure où les faits sont clairs, respectivement indubitables, de sorte qu'en cas de mise en accusation ceux-ci soient très probablement constatés de la même manière par le juge du fond. Tel n'est pas le cas lorsqu'une appréciation différente par le juge du fond apparaît tout aussi vraisemblable. Le principe « *in dubio pro duriore* » interdit ainsi au ministère public, confronté à des preuves non claires, d'anticiper sur l'appréciation des preuves par le juge du fond. L'appréciation juridique des faits doit en effet être effectuée sur la base d'un état de fait établi en vertu du principe « *in dubio pro duriore* », soit sur la base de faits clairs (ATF 143 IV 241 consid. 2.3.2 p. 244 et les références citées; cf. récemment arrêt du Tribunal fédéral 6B_1276/2019 du 27 février 2020 consid. 3.1 et la référence citée).

4.1.3 En vertu de l'art. 6 al. 1 CPP, les autorités pénales recherchent d'office tous les faits pertinents pour la qualification de l'acte et le jugement du prévenu (maxime de l'instruction). Par ailleurs, selon l'art. 7 al. 1 CPP, elles sont tenues, dans les limites de leurs compétences, d'ouvrir et de conduire une procédure lorsqu'elles ont connaissance d'infractions ou d'indices permettant de présumer l'existence d'infractions (principe du caractère impératif de la poursuite).

4.2 A teneur de l'art. 143 al. 1 CP, se rend coupable de soustraction de données 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.

Les données informatiques doivent avoir une protection spéciale – au moyen de mesures techniques, et non seulement en raison d'obstacles légaux, moraux ou contractuels – démontrant la volonté de la personne ayant légalement accès aux données d'empêcher que des tiers n'accèdent à ses données ou de restreindre cet accès. La personne non autorisée doit pouvoir reconnaître que les données sont protégées. 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 norme pénale ne s'applique donc pas à une attaque contre des données non protégées ou à leur utilisation illicite. Enfin, il n'est pas exigé que le propriétaire possède de meilleures compétences informatiques que l'auteur, ni que la protection ait une efficacité particulière (TPF 2016 28 consid. 2.1 et les références citées).

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. 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 (TPF 2016 28 consid. 2.1 et les références citées).

4.3 Les griefs des parties sont les suivants:

4.3.1 Les recourants rappellent le contexte global de leur plainte pénale, à savoir que les données en question n'appartenaient pas à D. et que celui-ci n'était initialement pas en leur possession. Ainsi, le MPC ne peut occulter la problématique de l'obtention préalable indue des données volées. En l'état, ils soutiennent qu'il existe des indices suffisants en mains du MPC en faveur de la commission d'une soustraction de données. D. a lui-même reconnu – ce que le MPC a ignoré – avoir obtenu une copie du serveur de B. SA. Cette version des faits expliquée par D. est contredite par l'informaticien F., qui fait état que D. avait les connaissance informatiques nécessaires afin de « hacker » les codes. Les recourants défendent ainsi qu'il est erroné de retenir, comme l'a fait le MPC, que les informations divulguées par D. provenaient exclusivement des boîtes e-mails de A. et E., dont D. aurait eu les mots de passe. La question n'a pas été instruite de savoir si D. disposait de mots de passe, dans quelles circonstances lesdits mots de passe lui auraient été confiés, ni à quel contenu ils auraient prétendument permis d'avoir accès. De plus, d'après les recourants, il ressort du vocabulaire adopté par le MPC que celui-ci admet que les données, dont D. était en possession, ne provenaient pas exclusivement des boîtes e-mails de A. et E. Le manque de clarté de la situation s'oppose déjà à la prise d'une décision de non-entrée en matière. De plus, la provenance des données soustraites et le moyen d'acquisition de ces données informatiques restent à ce stade inconnu, de sorte que le MPC est tenu d'enquêter et ne peut se contenter de son unique interprétation des faits. Ainsi, à défaut d'investigations supplémentaires, il est prématuré de retenir l'absence d'accès indu en tant qu'élément constitutif de l'infraction de soustraction de données (art. 143 CP). Les recourants avancent la thèse la plus plausible, selon eux, que D. a accédé et copié, par piratage du système informatique, l'intégralité des données du serveur du groupe C., qui contenait des informations confidentielles et dont l'accès était protégé, et ce indépendamment de l'accès qu'il avait aux boîtes e-mails de A. et E. Enfin, les recourants soulèvent qu'un tel examen n'est pas négligeable, dès lors que les données obtenues illicitement de B. SA ont été notamment versées à la procédure pénale ouverte contre A. et E., alors qu'elles seraient inexploitables ainsi que toutes les preuves dites « dérivées » (act. 1, 13 et 17).

4.3.2 Le MPC soutient que l'élément constitutif objectif des *données spécialement*

protégées fait défaut, puisque « D. était précisément en possession des mots de passe des ordinateurs de A. et E. ». Selon le MPC, les deux rapports, soit celui du 19 juin 2015 préparé par la société G. et celui du 24 mars 2015 préparé par la société H., démontrent que D. a bien transféré un grand nombre d'informations provenant de la société B. SA, notamment en ayant eu accès à la boîte mail de A. et E., dont il avait les mots de passe. Le MPC se réfère au « *written statement* » de E. devant la police thaïlandaise qui a fait mention d'un courriel reçu de D. dans lequel ce dernier indiquait être principalement en possession des courriels de A. et E. De plus, les faits parus dans le « *I.* » se basent principalement sur le contenu des courriers auxquels D. avait accès. Enfin, le MPC souligne qu'il n'apparaît nulle part que le reste des données volées provenant du serveur de B. SA était protégé par des mots de passe (act. 1.1, 4 et 15).

4.4 A titre liminaire, il sied de rappeler les relations entre les différents protagonistes. D. a été engagé auprès de la société B. SA aux alentours des années 2007 et 2009, de sorte qu'il était employé de cette société. A. est l'administrateur président de la société B. SA avec signature individuelle (cf. registre du commerce) et se présente comme le « fondateur et le *Chief Executive Officer* » du groupe C. (act. 1 n. 7). Au moment des faits, soit lors de la potentielle soustraction de données au printemps 2011, E. travaillait également au sein de B. SA: les recourants s'y réfèrent comme l' « ancien *Chief Investment Officer* de B. SA » et, selon le registre du commerce, il a été un administrateur de B. SA, avec signature collective à deux, de juin 2011 à mai 2018 (act. 1 n. 7). B. SA et D. ont résilié avec effet immédiat leur relation contractuelle au 15 avril 2011 (« *employment agreement* » act. 1.4 annexes 7 [le document n'est pas signé par les parties, mais selon les recourants il reflète leur accord, dès lors qu'ils s'étaient intégralement entendus sur les termes]; « *termination agreement* » act. 1.4 annexe 5; audition de D. du 23 février 2017 en qualité de personne à donner des renseignements dans la procédure pénale n. SV.15.0969: act. 1.10).

En outre, afin d'avoir une conception claire du contexte dans lequel intervient le présent recours, il sied d'énumérer les différentes procédures pénales topiques ouvertes devant le MPC. Par ordonnance d'ouverture d'instruction du 13 août 2015 et ordonnance d'extension du 14 août 2015, le MPC a, suite aux dénonciations MROS, ouvert une procédure pénale contre deux anciens agents publics malaisiens, sous le numéro de procédure SV.15.0969. L'ouverture de cette instruction pénale serait une conséquence de la révélation dans la presse des données de B. SA, dont D. était en possession (recours act. 1 n. 15 à 16). Le MPC a ouvert le 8 décembre 2017 une nouvelle instruction pénale (n. SV.17.1802) contre A. et E. pour, notamment, soupçons de gestion déloyale (art. 158 CP), escroquerie par métier (art. 146 al. 1 et 2 CP), corruption active d'agents publics étrangers (art. 322^{septies} al. 1

CP), faux dans les titres (art. 251 CP) et blanchiment d'argent aggravé (art. 305bis ch. 1 et 2 CP). Enfin, le présent recours a été interjeté dans le cadre de la procédure pénale n. SV.18.0492 ouverte contre D. pour service de renseignements économiques au sens de l'art. 273 CP (cf. let. B).

4.5

4.5.1 En l'espèce, les écritures des recourants documentent peu sur la gestion du parc informatique de B. SA, de la configuration des appareils ou encore des procédés techniques (physique ou électronique). La gestion des données en lien avec les employés de la société n'est également pas abordée. Ainsi, non seulement l'argumentation développée par les recourants se limite à des généralités en se contentant d'affirmer que les données étaient protégées au moyen de mots de passe, mais de plus révèle des contradictions. D'une part, les recourants exposent qu'une protection avait été effectivement mise en place interdisant l'accès des données à D., mais d'autre part ils soutiennent que la procédure pénale devrait encore être instruite sur la manière dont D. a eu accès à ces données. Dans la mesure où ils allèguent que leurs propres données auraient été « volées », il appartiendrait à A. et B. SA eux-mêmes de répondre à ces questions. En outre, on peine à discerner quel acte concret d'instruction permettrait de fournir de plus amples informations, autres que les concernés, étant rappelé que la société B. SA gère son parc informatique, dont ils revendiquent désormais le « hackage ». Les recourants ne suggèrent d'ailleurs pas à quel complément d'instruction devrait procéder le MPC. Il n'apparaît donc pas qu'il existerait des éléments matériels permettant de retenir que les données obtenues par D. étaient spécialement protégées contre un accès indu, étant rappelé que D. était employé de B. SA et non un quelconque tiers.

Il ressort encore du dossier plusieurs éléments relatifs à l'éventuelle soustraction des données opérée par D., notamment en rapport avec la question de savoir si les données étaient spécialement protégées. Il convient donc de les examiner.

4.5.2 A l'appui de leur thèse, les recourants ont produit deux rapports, l'un de la société G. du 19 juin 2015 (act. 1.4 annexe 1) et le second de H. du 24 mars 2015 (act. 1.4 annexe 2). Ces rapports portent sur la boîte e-mail et l'ordinateur professionnels de D. Ces rapports attestent notamment que D. aurait enregistré des données sensibles de B. SA sur Dropbox (act. 1.4 annexe 2 p. 2 et 14), qu'il aurait transféré des données entre ses boîtes e-mail professionnelle et privée (act. 1.4 annexe 1 n. 4 et 23), que les documents envoyés par D. lors des faits de chantage n'apparaitraient pas sur les documents qu'il s'est auto-envoyés (act. 1.4 annexe 1 n. 4 et 25), que dans les vingt-quatre heures précédant son départ, D. aurait connecté des clés USB et un Blackberry à son ordinateur de la société (act. 1.4 annexe 1

n. 4, 16, 19 et 20) ou encore que les dossiers de B. SA auraient pu être copiés subrepticement en utilisant la « B. SA LAN » via l'ordinateur de E. (act 1.4 annexe 2 p. 2 et 5).

Comme l'a soulevé à juste titre le MPC, ces rapports diligentés par les recourants, ou même E., n'apportent pas plus d'éclaircissements sur les mesures de sécurité mises en place au sein de la société B. SA ni sur la protection que D. aurait dû surmonter pour avoir accès aux données. Ces rapports ne constituent donc pas des éléments matériels démontrant que les données étaient spécialement protégées.

4.5.3 En 2015, D. a été condamné par la justice thaïlandaise à une peine privative de trois ans pour des faits de chantage (act. 1.4 annexe 4). Il ressort du jugement thaïlandais que, entre le 22 juillet 2013 et le 17 octobre 2013, soit après la fin des rapports de travail, D. a menacé E. de révéler les informations confidentielles de la société B. SA, s'il ne lui versait pas une certaine somme. Cette condamnation s'est fondée notamment sur un échange d'e-mails intervenu en 2013 entre D. et ses ex-employeurs (A. et E.). Aux termes de l'un de ces e-mails, D. a indiqué: « j'ai en ma possession tous les détails, même les plus importants, des débuts de B. SA jusqu'à mon départ. Ce sont plusieurs milliers de documents, principalement des e-mails. […] Les dernières semaines avant mon départ de Londres, j'ai été tellement mal traité et même plus que cela que j'ai dû me protéger en prenant ce que j'appellerais une assurance-vie », act. 1.4 annexe 6). Par ailleurs, dans le cadre de cette procédure pénale thaïlandaise, E. a indiqué à la police thaïlandaise comment D. avait eu accès aux informations de la société (« *written statement of the Petitioner, Complainant or Witness* » du 8 mai 2015, p. 8): « *In addition to his responsibility for information technology management in the Company, Mr. D. specifically assisted Mr. A. and me. For example, if we traveled abroad for business purposes and wanted to have some documents to be sent to our computers. This was normally in accordance with the principle of a specific action for each time under the express understanding that Mr. D. would be able to access our computers when he was assigned to do so for the specific purposes only. In order for Mr. D. to perform his duties, it was necessary for him to access Mr. A.'s and my computer (in accordance with the specific purpose for each time and under the express understanding only). Therefore, we gave him our password* » (act. 1.4 annexe 3).

Au vu de ces éléments, D. aurait eu le mot de passe de A. et E. pour accéder à leur ordinateur (« *computer* »). Certes, une protection spéciale (mot de passe) avait été mise en place, néanmoins elle ne s'appliquait pas à D. La seule barrière pour D. était d'être limitée aux seules instructions données par A. et E., ce qui ne constitue pas des mesures de sécurité suffisantes au sens

de l'art. 143 CP. Dans cette constellation, la condition objective de protection spéciale des données contre un accès indu de D. ne serait pas réalisée. Les déclarations de E. contredisent la thèse des recourants selon laquelle D. aurait piraté le système informatique de B. SA (v. consid. 4.3.1). Les recourants n'apportent guère d'explications sur ces déclarations de E., qui travaillait également pour B. SA au moment des faits. Enfin, le récit de E., ou celui des recourants, s'oppose diamétralement aux déclarations de D. ou de F. (v. ci-dessous consid. 4.5.4).

4.5.4 Il sied encore d'examiner les déclarations de D. en 2017 selon lesquelles le contenu du serveur du groupe Bb. SA lui aurait été remis par l'informaticien de cette société par amitié (audition de D. du 23 février 2017 en qualité de personne à donner des renseignements dans la procédure pénale n. SV.15.0969 [act. 1.10]). D. a expliqué: « Je me suis également occupé de la supervision de l'installation de tout le parc informatique de B. SA, étant précisé que les serveurs se trouvaient à Genève (p. 3). […] Pour ce faire j'ai travaillé avec F. qui exploitait une société informatique basée en Valais (p. 4) […] sauf erreur en mai ou en juin 2011, j'ai voulu avoir une assurance au cas où, raison pour laquelle j'ai contacté l'informaticien F., avec qui j'avais travaillé pour la mise en place du parc informatique de B. SA et je lui ai demandé si par amitié me mettre à disposition une copie du serveur de B. SA. F. a accepté de me rendre ce service et il m'a donc remis une copie du serveur de B. SA en me précisant que le serveur avait été détruit ou les données effacées sur ordre de A. Je pense que F. avait dû garder une copie du serveur car sans cela il n'aurait pas pu m'en remettre un exemplaire vu cette destruction ou cet effacement de données » (p. 6 à 7). L'informaticien F. a quant à lui réfuté les déclarations de D. et de lui avoir remis « quoique ce soit » (act. 1.11 p. 5 audition de F. en qualité de personne appelée à donner des renseignements du 31 mars 2017 dans le cadre de la procédure pénale n. SV.15.0969). En audition de confrontation du 5 juillet 2017, les deux intéressés ont confirmé leurs déclarations respectives sans permettre de clarifier les faits (act. 1.13).

Certes, comme soulevé par les recourants, le MPC n'a pas mentionné les auditions précitées dans la décision entreprise. Toutefois, on comprend que le MPC a retenu que celles-ci n'influençaient pas son appréciation. Les deux intéressés, D. et F., ayant été confrontés sans résultat, l'on ne discerne pas au vu du dossier ce qui permettrait de retenir l'une de ces déclarations plus qu'une autre, ou quelle mesure d'instruction permettrait de le faire. De surcroît, comme il l'a déjà été abordé précédemment, il s'agit de versions qui s'opposent à celle présentée par les recourants (v. consid. 4.3.1) ou à celle de E. devant les autorités thaïlandaises (v. consid. 4.5.3). La Cour constate que le dossier comprend autant de versions que de personnes impliquées. En l'absence d'éléments matériels suffisants fournis par B. SA, titulaire des

données sur la sécurité de son parc informatique, ou par A. sur la gestion sécuritaire de ce parc, force est de constater que des déclarations contradictoires s'opposent sans permettre de retenir une version plutôt qu'une autre.

4.5.5 Les recourants produisent encore un article de presse paru le 19 novembre 2019 dans un média suisse, lequel contient une interview récente de J. Ils expliquent qu'elle a rédigé, en tant qu'intervenante principale, des articles sur « I. » en lien avec les faits de la cause et peut être considérée comme l'interlocutrice privilégiée de D. Les recourants font ainsi référence au passage suivant de son interview: *« 2014 kam ein Whistleblower, ein Ex-Manager des Ölkonzerns B. SA, der schon 2009 mit 1MDB ein Joint Venture gegründet hatte. Der Mann hatte reichlich Material, unter anderem Hunderttausende E-mails, von den Servern kopiert* » (act. 13.1 p. 3). D'après les recourants, de par la connaissance étendue de la situation qu'avait J., sa déclaration permet de confirmer que D. a soustrait de manière indue les éléments du serveur de B. SA en les copiant (réplique act. 13 n. 4 à 7). La Cour de céans ne voit pas les éléments qu'une journaliste en tant que témoin indirect pourrait apporter qui ne figureraient pas déjà au dossier. Un tel grief doit être écarté.

4.5.6 Les recourants défendent encore que D. se serait engagé contractuellement à une utilisation diligente et précautionneuse des moyens de communication et appareils électroniques et à garder confidentielle toute information en lien avec le groupe Bb. Cette dernière obligation aurait vocation à s'appliquer également au-delà de la fin de ses rapports de travail. Il aurait garanti n'avoir gardé aucun document, support ou copies de ces derniers contenant des données confidentielles (cf. act. 1.4 n. 32, 38 et 39 et les annexes citées). Il sied de souligner que de telles clauses contractuelles ne permettent pas de protéger des données contre un accès indu au sens de l'art. 143 al. 1 CP (v. consid. 4.2). L'accès doit être interdit au moyen de mesures techniques, ce qu'une interdiction contractuelle n'est pas. Ce grief doit également être écarté.

4.5.7 A titre superfétatoire, il sied de relever que le vocabulaire utilisé par le MPC pour définir les données, dont D. a été en possession, ne constitue pas un élément permettant de démontrer que l'infraction de soustraction de données (art. 143 CP) est réalisée. En d'autres termes, il n'est pas pertinent pour l'examen de l'énoncé de fait légal que le MPC fasse état dans une demande de ressource à la Police judiciaire fédérale du 13 août 2015 que des données informatiques ont été « volées » par D. (cf. act. 1 n. 16 en lien avec l'act. 1.5) ou que dans un document la Procureure fédérale en charge de la procédure n. SV.17.1802 fasse référence à la jurisprudence relative à des « données obtenues illicitement par des particuliers » (act. 24 n. 2 en

lien avec l'act. 19.1).

4.5.8 Vu l'objet du présent recours, il n'y a pas lieu d'entrer en matière sur la lettre du MPC du 30 avril 2020 faisant part – dans la procédure pénale ouverte contre A. et E. référencée sous le n. SV.17.1802 – de la volonté de procéder à l'exploitation des données litigieuses *in casu* (v. let. F). Cette lettre a d'ailleurs donné lieu à un recours auprès de la Cour de céans. Dans la mesure où les griefs des recourants auraient eu trait au présent recours, ceux-ci ont été développés ci-dessus. Pour les mêmes motifs, il n'y a pas lieu de donner suite à la requête des recourants (act. 24 n. 1) sollicitant l'interpellation des Procureurs fédéraux en charge des procédures n. SV.17.1802 et n. SV.18.0492, pour avoir des précisions utiles sur les échanges intervenus entre eux en lien avec les observations déposées le 20 mai 2020 devant la Cour de céans, suite à la lettre du MPC du 30 avril 2020 (v. let. F).

4.5.9 En résumé, le MPC a déterminé que les données dont D. avait eu accès étaient principalement issues des boîtes e-mail de A. et E., dont D. avait les mots de passe. Le MPC a apprécié les éléments au dossier et les déclarations des parties pour établir les faits, bien qu'aucune instruction n'ait encore été ouverte. Il a fait une fausse application du principe « *in dubio pro duriore* » en procédant en réalité à une appréciation des preuves qui relève de la compétence du juge du fond. Toutefois, la décision du MPC de refus d'étendre l'instruction doit être confirmée au motif que les déclarations contradictoires s'opposent sans éléments matériels permettant de retenir une version plutôt qu'une autre. Ainsi, au vu des éléments du dossier, les recourants ne rendent pas l'existence de faits pénalement répréhensibles au regard de l'art. 143 CP (notamment l'existence d'une protection spéciale) plus vraisemblable ou tout au moins aussi vraisemblable qu'un acquittement.

4.6 Il s'ensuit que le recours portant sur l'extension de l'instruction doit être rejeté dans la mesure de sa recevabilité.

Refus d'admission de partie plaignante

5. Les recourants disposent de la qualité pour recourir contre la décision du MPC de lui refuser l'admission de la qualité de partie plaignante dans le cadre de la procédure menée par le MPC. En effet, la décision entreprise lèse les recourants dans leur intérêt juridiquement protégé, en tant qu'ils sont exclus de la procédure (arrêt du Tribunal pénal fédéral BB.2012.18-23 du 22 novembre 2012 consid. 2.1).

6. Sur le fond, il sied de distinguer l'admission de la partie plaignante dans le

cadre de l'art. 143 ou de l'art. 273 CP.

6.1 Concernant l'art. 143 CP, il sied de relever que le MPC a refusé à juste titre d'étendre l'instruction à cette infraction et à ce sujet les recourants ont eu la possibilité d'être entendus dans le cadre de cette procédure devant une autorité avec plein pouvoir d'examen (v. *supra* consid. 1.2). Par conséquent, la question ne mérite pas d'être approfondie (v. *supra* consid. 4).

6.2 Les recourants ne revêtent pas la qualité de partie plaignante eu égard à l'art. 273 CP (cf. notion de partie plaignante *supra* consid 3.1).

6.2.1 Lorsque l'infraction protège en première ligne l'intérêt collectif, les particuliers ne sont considérés comme des lésés que si leurs intérêts privés ont été effectivement touchés par les actes en cause, de sorte que l'atteinte apparaît comme la conséquence directe de l'acte dénoncé (ATF 141 IV 454 consid. 2.3.1; 138 IV 258 consid. 2.3; 123 IV 183 consid. 1c; 119 Ia 342 consid. 2b; arrêts du Tribunal fédéral 1B_261/2017 du 17 octobre 2017 consid. 3; 6B_402/2016 du 28 novembre 2017 consid. 1.2; arrêt du Tribunal pénal fédéral BB.2012.67 du 22 janvier 2013 consid. 1.3).

6.2.2 S'agissant des services de renseignements économiques (art. 273 CP), le bien juridique protégé est les intérêts publics (décision du Tribunal pénal fédéral BB.2013.177 du 26 mars 2014 consid. 1.3.2 et les références citées). Les intérêts économiques des personnes ou entreprises installées en Suisse sont quant à eux protégés de façon secondaire. Cette disposition n'a pas été édictée dans l'optique de protéger des intérêts privés, ceux-ci étant pris en considération par l'art. 162 CP (violation du secret de fabrication ou du secret commercial). En conséquence, un particulier n'est pas le titulaire du bien juridique protégé.

6.2.3 En l'occurrence, les recourants se prévalent, en tant que dommage découlant des actes qu'ils dénoncent, qu'ils ne seront pas à même de défendre leurs droits, notamment ceux relatifs à la problématique de preuves illicites dans la présente procédure et la procédure n. SV.15.0969 menée par le MPC (act. 1 n. 75). Ce dommage n'apparaît pas comme la conséquence directe de l'acte dénoncé, de sorte qu'ils ne peuvent être légitimés en tant que partie plaignante.

6.3 Concernant le refus d'admission de partie plaignante, le recours est également mal fondé et par conséquent rejeté.

7. En tant que parties qui succombent, les recourants supporteront solidairement les frais de la présente procédure (cf. art. 428 al. 1 CPP). Ceux-ci se limitent en l'espèce à un émolument qui sera fixé à CHF 4'000.--

en application des art. 5 et 8 al. 1 du règlement du Tribunal pénal fédéral du 31 août 2010 sur les frais, émoluments, dépens et indemnités de la procédure pénale fédérale (RFPPF; RS 173.713.162).

Par ces motifs, la Cour des plaintes prononce:

1. Le recours est rejeté dans la mesure de sa recevabilité.

2. Un émolument de CHF 4'000.-- est mis à la charge solidaire des recourants.

Bellinzone, le 26 janvier 2021

Au nom de la Cour des plaintes
du Tribunal pénal fédéral

Le président: La greffière:

Distribution

- Mes Myriam Fehr-Alaoui, Jean-François Ducrest, Paolo Bernasconi et Daniel Zappelli, avocats
- Ministère public de la Confédération

Indication des voies de recours

Il n'existe pas de voies de recours ordinaire contre la présente décision.