Bundesstrafgericht
Tribunal pénal fédéral
Tribunale penale federale
Tribunal penal federal

Numéro du dossier: SK.2024.24

Jugement du 16 avril 2025
Cour des affaires pénales

Composition

Les juges pénaux fédéraux
Stephan Zenger, juge président,
Stefan Heimgartner et Maric Demont
la greffière Alexandra Mraz

Parties

MINISTÈRE PUBLIC DE LA CONFÉDÉRATION,
représenté par le Procureur fédéral Yves Nicolet et le Procureur fédéral a.i. Jean-Philippe Peissard

et les parties plaignantes :

1. **B.,** représentée par Me Sébastien Fanti,

2. **C.,** représentée par Me Serge Fasel,

3. **D.,** représentée par Me Benjamin Borsodi et Me Charles Goumaz,

4. **E.,**

5. **F.,** représentée par Me Benjamin Borsodi et Me Charles Goumaz,

6. **G.,** représentée par Me Christophe de Kalbermatten,

7. **H.,** représentée par Me Cédric Page,

8. I.,

9. J.,

10. K.,

11. L.,

12. M.,

13. N.,

14. O.,

15. P.,

16. Q.,

17. R.,

contre

A., de nationalité française et israélienne, défendu par Me Marc Bonnant

Objet

Soustraction de données (art. 143 CP), accès indu à un système informatique (art. 143bis CP), utilisation frauduleuse d'un ordinateur par métier (art. 147 al. 1 et 2 CP)

Procédure

A. Devant le Ministère public de la Confédération

A.1 En date du 10 mars 2021, le Ministère public de la Confédération (ci-après : le MPC) a étendu à A. son instruction n° SV.17.0837 diligentée contre inconnu pour des cas de *social engineering* du type « arnaque au faux technicien bancaire », commis au préjudice de nombreuses sociétés suisses, entre la fin de l'année 2016 et l'été 2018 (MPC 01-01-0021). L'instruction n° SV.17.0837 a plus précisément porté sur des soupçons de soustraction de données (art. 143 CP), accès indu à un système informatique (art. 143bis CP), utilisation frauduleuse d'un ordinateur par métier (art. 147 al. 2 CP), éventuellement escroquerie et tentative d'escroquerie (art. 146 et 146 CP en lien avec l'art. 22 CP) et blanchiment d'argent qualifié (art. 305bis al. 1 et 2 lit. a et c CP ; MPC 01-01-0021 et 01-01-0024).

A.2 Il ressortait en effet de mesures d'instruction effectuées en Israël, par voie d'entraide, que A. (ci-après également : le prévenu) était l'utilisateur du raccordement +1, sur lequel étaient déviés tous les appels entrants sur les numéros +2 et +3, au moyen desquels les auteurs des fraudes avaient effectué de nombreux appels aux sociétés suisses lésées, ceci depuis Israël (MPC 01-01-0021). Ainsi, à teneur de la réponse des autorités israéliennes à la commission rogatoire du MPC (MPC 18-02-0057 ss), A. était le titulaire du raccordement israélien en question (MPC 18-02-0058). De plus il ressortait des mesures d'investigation israéliennes que l'appareil utilisé pour le raccordement +1 avait pu être géolocalisé à plusieurs reprises au même endroit qu'un autre appareil également attribué à A., à savoir celui utilisé avec le raccordement +4 (MPC 18-02-0058 et 18-02-0069). Enfin, les autorités israéliennes avaient procédé à une surveillance active des numéros +1 et +4 (MPC 18-02-0058), ainsi qu'à une comparaison de voix des utilisateurs desdits raccordements, arrivant à la conclusion qu'il s'agissait d'une seule et même personne (MPC 18-02-0058, 18-02-0064 et 18-02-0071).

A.3 Par ordonnance du 28 février 2022, le Tribunal des mesures de contrainte du canton de Vaud (ci-après : Tmc VD) a autorisé l'exploitation, à l'encontre de A., des données issues de surveillances rétroactives des raccordements 5 (autorisation originale référencée Tmc PC17.025361-CPB ; MPC 09-01-0009), 6 (autorisation originale référencée Tmc PC17.025361-CPB ; MPC 09-021-0009), 6 (autorisation originale référencée Tmc PC18.014789-CPB ; MPC 09-02-0016), 7 (autorisation originale référencée Tmc PC18.009815-SDE ; MPC 09-03-0010) et 8 (autorisation originale référencée Tmc PC19.002329-PHK ; MPC 09-07-0041) ainsi que de surveillances actives des raccordements 3 (autorisation originale référencée Tmc PC18.010610-SDE ; MPC 09-04-0022), 9 (autorisation originale référencée Tmc PC18.011602-CPB; MPC 09-05-0018), 2 (autorisation originale référencée Tmc PC18.012896-CPB ; MPC 09-06-0018) et 8

(autorisation originale référencée Tmc PC18.020801-CPB ; MPC 09-07-0009), toutes effectuées antérieurement à l'extension de l'instruction à A. (MPC 09-08-0020 ss).

A.4 Suite à son signalement international et son arrestation aux Etats-Unis dans la nuit du 31 janvier 2022, A. a été extradé vers la Suisse le 20 avril 2022 et placé en détention provisoire, pour une période initiale de 3 mois, au motif d'un risque de fuite notamment (MPC 06-01-0014, 06-01-0197, 06-01-0116, 06-01-0119 et 06-01-0209 ss). Prolongée par deux fois, la détention provisoire a, par ordonnance du 12 décembre 2022, fait l'objet de mesures de substitution (MPC 06-01-0282 ss, 06-01-0316 ss et 06-01-346 ss). A. s'est ainsi engagé à fournir des sûretés par CHF 250'000.-, ainsi qu'à rester à la disposition des autorités pénales suisses et élire un domicile de notification en l'étude de son conseil principal de l'époque, Me Laurent Moreillon (MPC 06-01-0349). Il a été libéré de détention le 14 décembre 2022, à 11h55 (MPC 06-01-0350 et 06-01-0360).

A.5 Au cours de sa détention provisoire, A. a été entendu à plusieurs reprises, soit les 21 avril 2022 (MPC 13-01-0001 ss), 29 avril 2022 (MPC 13-01-0012 ss), 6 mai 2022 (MPC 13-01-0039 ss), 22 juin 2022 (MPC 13-01-0057 ss), 29 juin 2022 (MPC 13-01-0084 ss), 15 juillet 2022 (MPC 13-01-0168 ss), 11 octobre 2022 (MPC 13-01-0184 ss), 28 octobre 2022 (MPC 13-01-0235 ss), 10 novembre 2022 (MPC 13-01-0253 ss), 30 novembre 2022 (MPC 13-01-0291 ss) et 7 décembre 2022 (MPC 13-01-0320 ss), ceci à chaque fois assisté d'un ou plusieurs défenseurs. Lors de ces auditions, le prévenu a notamment été confronté à différents moyens de preuve qui, pour partie, avaient été administrés préalablement à l'ouverture d'instruction à son égard, ainsi qu'à son extradition vers la Suisse. En tant que besoin, il sera revenu ci-après sur les déclarations du prévenu et les moyens de preuve qui lui ont été présentés.

A.6 Parallèlement, le MPC a procédé à des investigations complémentaires par voie d'entraide internationale avec Israël notamment (MPC rubrique 18), dont la perquisition du domicile du prévenu (MPC 18-02-0072 ss) et mandaté la société 1 pour effectuer une expertise technique de la voix de A. par mandat du 31 mai 2022 (MPC rubrique 11).

A.7 Il sied en outre de préciser que de nombreux autres moyens de preuves ont été administrés, dans le contexte de la procédure préliminaire, préalablement à l'identification de A. et l'extension de l'instruction à sa personne.

A.8 Ainsi, en particulier, il a été procédé, entre 2017 et 2020, à des commissions rogatoires internationales près les autorités judiciaires d'Allemagne (MPC 05-12-0068 ss, 05-12-0101 ss et 05-12-0068-0172 ss ; rubriques 18.01, 18.17 à 18.19), d'Israël (MPC rubrique 18.02), de France (MPC rubrique 18.03), des Etats-Unis (MPC rubrique 18.04), de Belgique (MPC rubrique 18.06), de Tchéquie

(MPC rubrique 18.07), des Pays-Bas (MPC 05-12-0101 ss ; rubrique 18.08), du Luxembourg (MPC rubrique 18.09), de la République populaire de Chine (MPC 05-02-0069 ss ; rubrique 18.10), d'Estonie (MPC rubrique 18.12), de Bulgarie (MPC rubrique 18.13), de Hongrie (MPC rubrique 18.14), du Royaume-Uni (MPC rubrique 18.15), de Pologne (MPC rubrique 18.16) et d'Autriche (MPC rubrique 18.20).

En outre, des demandes de productions et de renseignements ont été effectuées, auprès de plusieurs établissements bancaires suisses (MPC 05-00-0073 ss, 05-00-0096, rubriques 07.02 et 07.04 s.) ainsi qu'auprès d'autres sociétés (MPC rubrique 07.06 ss). Le MPC a également procédé à des perquisitions (MPC rubrique 08) ainsi qu'à l'audition de parties plaignantes et de témoins (MPC rubrique 12).

A.9 L'enquête a aussi permis d'obtenir le blocage d'une partie des fonds délictueux en vue de leur rapatriement en faveur des sociétés lésées. Elle a ainsi notamment permis de séquestrer une partie du produit du crime au préjudice de B. sur la relation de la société 2 auprès de la banque 1 à Genève, soit CHF 42'645.86, puis GBP 253'685.41 avec valeur à CHF 247'416.95 au 30 juin 2021 (MPC 07-03-0039 et 07-03-0209). En application des art. 267 CPP et art. 70 al. 1 CP, les fonds ont d'ores et déjà été restitués à la lésée en cours d'instruction, par ordonnances des 30 juin 2017 et 21 septembre 2021 (MPC 07-03-0001 ss et 07-03-0211 ss), soit CHF 42'645.86 le 18 juillet 2017 (SK 37.551.035) puis CHF 314'729.72 le 21 octobre 2021 (SK 37.551.037).

En l'état, aucune mesure de séquestre n'est en cours (acte d'accusation du 4 avril 2024 et dossier du MPC *a contrario*).

A.10 La Police judiciaire fédérale (ci-après : PJF) a rendu son rapport final le 30 mars 2023 (MPC 10-08-0004 ss) précédé de plusieurs rapports antérieurs dont, en particulier, le rapport du 7 novembre 2018 concernant l'exploitation de contrôles téléphoniques actifs (MPC 10-02-0195 ss), les rapports d'analyse et évaluation des données informatiques des 6 décembre 2018 (MPC 10-02-0302 ss) et 4 février 2019 (MPC 10-02-0334 ss) et les rapports des 30 juillet 2021 (MPC 10-02-0354 ss) et 26 août 2022 (MPC 10-05-0015 ss) relatifs à A.

A.11 Le 16 novembre 2023, le MPC a avisé les parties de la prochaine clôture de la procédure préliminaire, les informant qu'à l'issue de celle-ci il entendait, d'une part, renvoyer en accusation A. et, d'autre part, rendre une ordonnance de classement s'agissant des autres auteurs demeurant inconnus, dès lors que l'instruction n'avait pas permis de les identifier (MPC 03-01-0001 ss). Parallèlement, le MPC a imparti un délai aux parties pour déposer leurs éventuelles réquisitions de preuve notamment.

A.12 Les parties n'ont formé aucune réquisition de preuve (MPC rubrique 15 s. *e contrario*).

A.13 Comme il l'avait annoncé, le MPC a classé la procédure s'agissant des auteurs restés non identifiés, par ordonnance du 6 mars 2024 (MPC 03-01-0005 ss). Dans ladite ordonnance, il a en outre précisé ne pas entendre inclure, dans l'acte d'accusation contre A., le volet concernant la société lésée 3, faute d'avoir pu établir l'implication de celui-ci dans les faits dénoncés par ladite société (MPC 03-01-0007). L'ordonnance de classement du 6 mars 2024 est entrée en force (MPC 03-01-0012).

A.14 Enfin, on relèvera que les sociétés suivantes, lésées par les actes reprochés à A., ont déposé plainte pénale au cours de la procédure préliminaire : G. (chiffre 1.3.1 de l'acte d'accusation), anciennement G.a. et G.b. (MPC 05-12-0206 ss), le 10 janvier 2017 (MPC 05-12-0036, 05-12-0094 et 05-12-0214), F. (chiffre 1.3.2 de l'acte d'accusation) le 9 janvier 2017 (MPC 05-02-0016), I. (chiffre 1.3.3. de l'acte d'accusation) le 5 janvier 2017 (MPC 05-02-0030), H. (chiffre 1.3.4 de l'acte d'accusation) le 17 janvier 2017 (MPC 05-05-0027 ss), K. (chiffre 1.3.5 de l'acte d'accusation) le 11 janvier 2017 (MPC 05-02-0050), B. (chiffre 1.3.6 de l'acte d'accusation) le 31 janvier 2017 (MPC 05-00-0027), R. (chiffre 1.3.7 de l'acte d'accusation) le 16 février 2018 (MPC 05-04-0001), N., anciennement N.a. (MPC 15-02-0004) (chiffre 1.3.8 de l'acte d'accusation) le 27 décembre 2017 (MPC 05-03-0001), C. (chiffre 1.3.9 de l'acte d'accusation) le 6 juin 2018 (MPC 05-06-0006), L. (chiffre 1.3.10 de l'acte d'accusation) le 11 juin 2018 (MPC 05-07-0001), D. (chiffre 1.3.11 de l'acte d'accusation) le 14 juin 2018 (MPC 05-08-0004), E. (chiffre 1.3.12 de l'acte d'accusation) le 21 juin 2018 (MPC 05-10-0002), O. (chiffre 1.3.13 de l'acte d'accusation) le 15 juin 2018 (MPC 05-09-0003), M. (chiffre 1.3.14 de l'acte d'accusation) le 28 juin 2018 (MPC 05-11-0003, 05-11-0006 et 15-08-0002 ss), P. (chiffre 1.3.15 de l'acte d'accusation) le 5 juillet 2018 (MPC 05-14-0003), J. (chiffre 1.3.23 de l'acte d'accusation) le 13 janvier 2017 (MPC 05-05-0062 et 05-05-0085) et Q. (chiffre 1.3.25 de l'acte d'accusation) le 28 mai 2018 (MPC 05-15-0003).

Les sociétés 4 (chiffre 1.3.16 de l'acte d'accusation), 5 (chiffre 1.3.17 de l'acte d'accusation), 6 (chiffre 1.3.18 de l'acte d'accusation), 2, aujourd'hui 2.a. (chiffre 1.3.19 de l'acte d'accusation), la société 7 (chiffre 1.3.20 de l'acte d'accusation), la société 8 (chiffre 1.3.21 de l'acte d'accusation), la société 39 (chiffre 1.3.22 de l'acte d'accusation) et la société 9, aujourd'hui 9.a. (chiffre 1.3.24 de l'acte d'accusation) n'ont, elles, pas porté plainte.

A.15 La caution de CHF 250'000.-, versée par A. en date du 13 décembre 2022, a produit intérêt et s'élevait, au 31 décembre 2024, au montant de CHF 252'966.05 (SK 37.510.011).

B. Devant la Cour des affaires pénales

B.1 Le 4 avril 2024 (SK 37.100.001 ss), le MPC a renvoyé en accusation A. pour soustraction de données (art. 143 CP), subsidiairement accès indu à un système informatique (art. 143bis CP), accès indu à un système informatique (art. 143bis al. 1 et 2 CP) et utilisation frauduleuse d'un ordinateur par métier (art. 147 al. 1 et 2 CP).

B.2 <u>De l'administration de moyens de preuve complémentaires et des conclusions civiles</u>

B.2.1 Le 2 mai 2024, la Cour de céans a indiqué aux parties qu'elle entendait procéder à l'administration d'office des extraits des casiers judiciaires suisse, français et israélien du prévenu, ainsi qu'à l'audition aux débats de ce dernier, quant à sa situation personnelle et les faits de l'accusation. Par le même acte, les parties ont été invitées à formuler leurs éventuelles offres de preuves et chiffrer ainsi que motiver leurs éventuelles conclusions civiles (SK 37.400.0001 s.).

B.2.2 Se référant à l'ordonnance précitée, la société G. a requis, par la plume de son mandataire Me Christophe de Kalbermatten, le remboursement de ses frais d'avocat à hauteur de CHF 13'881.20, par courrier du 28 mai 2024 (SK 37.557.001 s.).

B.2.3 Par courrier du 29 mai 2024, la société C., agissant par Me Serge Fasel, a confirmé maintenir les conclusions civiles chiffrées prises par-devant l'autorité d'instruction et s'élevant à la somme d'EUR 920'975.-, soit CHF 970'049.-. Elle a en outre requis l'octroi d'une indemnité pour ses frais de représentation en justice par CHF 32'224.35, sous réserve de conclusions augmentées des opérations à venir, et produit des notes d'honoraires à l'appui de ladite requête (SK 37.552.001 ss).

B.2.4 Le 5 juillet 2024, B., agissant par l'intermédiaire de ses conseils Me Sébastien Fanti et Me Alexandre Staeger a conclu, principalement, à l'admission de ses conclusions civiles, la condamnation de A. au paiement, à la société B., des sommes de CHF 990'097.40 avec intérêts à 5% l'an dès le 27 janvier 2017, CHF 891.- avec intérêts à 5% l'an dès le 12 juin 2017 et CHF 45'407.85 avec intérêts à 5% l'an dès le 7 août 2017, sous suite de frais et dépens. Subsidiairement, B. conclut à l'admission de ses conclusions civiles, la condamnation de A. au paiement, à la société B., des sommes de CHF 364'775.42 avec intérêts à 5% l'an dès le 27 janvier 2017, EUR 574'492.74 avec intérêts à 5% l'an dès le 27 janvier 2017, CHF 891.- avec intérêts à 5% l'an dès le 12 juin 2017 et CHF 45'407.85 avec intérêts à 5% l'an dès le 7 août 2017, sous suite de frais et dépens. A l'appui de ses conclusions civiles, B. invoque les preuves administrées d'office telles que mentionnées dans l'ordonnance du 2 mai 2024, les éléments du dossier cités dans l'acte d'accusation en pages 11

et 12 sous notes de bas de page n° 25 à 29, les pièces déposées en annexe à son écriture du 5 juillet 2024 ainsi que l'audition des parties (SK 37.551.0001 ss).

B.2.5 Hormis G., C. et B., les autres parties n'ont pas formulé de réquisitions de preuve, ni formé de conclusions civiles, dans le délai que la Cour leur avait imparti par ordonnance du 2 mai 2024 pour ce faire.

B.2.6 Le 16 juillet 2024, la Cour de céans a rendu une ordonnance concernant les moyens de preuve, par laquelle elle a confirmé procéder aux administrations de preuve annoncées le 2 mai 2024 (cf. ch. B.2.1 *supra* ; SK 37.250.001 s.).

Elle a en outre versé au dossier, comme moyens de preuve, les pièces produites par G., C. et B. à l'appui de leurs conclusions civiles respectives (SK 37.250.001 ss).

B.2.7 La Cour a obtenu et versé au dossier les casiers judiciaires actualisés suisse et français de A. Bien qu'elle ait également entrepris les démarches nécessaires à l'obtention de son casier judiciaire israélien, ce dernier n'a pas été remis à la Cour (SK 37.231.1.001 ss et SK.37.720.005).

B.2.8 Par courrier du 3 mars 2025, Me Miriam Mazou a requis, pour le compte de A., que l'épouse de ce dernier, S., soit entendue comme témoin lors des débats (SK 37.521.005). Invitée à préciser les motifs de cette requête, Me Miriam Mazou a indiqué que S. serait à même de témoigner de la bonne moralité du prévenu et de sa vie de famille en Israël, ainsi que d'apporter un éclairage sur sa personnalité (SK 37.521.007). La Cour a rejeté cette offre de preuve le 17 mars 2025, le témoignage de S. n'apparaissant pas nécessaire, en sus de l'audition du prévenu, pour que la défense renseigne la Cour sur ces aspects (SK 37.400.046).

B.3 <u>De la qualité de partie des sociétés 3 et 10</u>

B.3.1 Parallèlement, par courrier du 31 mai 2024, la Cour de céans a interpellé le MPC quant au statut procédural des sociétés 3 et 10, indiquées comme partie plaignante dans l'acte d'accusation, alors que la description des actes reprochés au prévenu dans ce dernier ne les mentionne pas (SK 37.400.003 s.).

B.3.2 Dans sa détermination du 13 juin 2024, le MPC a confirmé à la Cour que les faits dénoncés par la société 3 et la société 10 ne font pas l'objet de l'acte d'accusation (SK 37.400.003 s.).

B.3.3 Par décisions séparées des 16 juillet 2024, la Cour a informé la société 3 et la société 10 qu'elle constatait que les sociétés ne revêtaient pas la qualité de partie à la présente procédure, de sorte qu'elle n'entendait pas les citer à participer aux débats, ni procéder à l'avenir à d'autres notifications en faveur desdites sociétés. Ces décisions, restées incontestées, sont entrées en force (SK 37.400.012 s.).

B.4 De la participation des parties à la procédure et aux débats

B.4.1 Parallèlement aux démarches précitées de la Cour, Me Lionel Halpérin l'a informée, par courrier du 11 juin 2024, qu'il cessait de représenter les intérêts du prévenu aux côtés de Me Miriam Mazou et que l'élection de domicile faite en son Etude était révoquée (SK 37.521.002). Pendant la suite de la procédure par-devant la Cour de céans, A. a continué d'être assisté de Me Miriam Mazou.

B.4.2 Toujours dans le contexte de la préparation des débats, la Cour a interpellé Me Miriam Mazou, le 16 juillet 2024, en vue d'obtenir confirmation que son mandant acceptait bien de se voir notifier sa citation personnelle à comparaître aux débats directement en l'Etude de sa mandataire, conformément aux engagements idoines pris par le prévenu lors de l'audition du 7 décembre 2022 (SK 37.400.011).

B.4.3 Par courrier du 26 juillet 2024, le prévenu, agissant par Me Miriam Mazou, a confirmé qu'il acceptait de se voir notifier sa citation personnelle à comparaître aux débats directement en l'Etude de sa mandataire. Me Miriam Mazou a en outre annoncé solliciter pour lui la délivrance d'un sauf-conduit pour comparaître aux débats (SK 37.521.003).

B.4.4 La Cour a par la suite informé les parties de la tenue des débats le 7 avril 2025 (SK 37.310.001 ss). Le 17 décembre 2024, elle a imparti aux parties plaignantes un délai pour lui communiquer si elles souhaitaient participer activement à la procédure et, le cas échéant, prendre part aux débats, leur indiquant que faute de réponse expresse de leur part, la Cour considérerait que les parties plaignantes renonçaient à ces droits et qu'elle ne leur adresserait alors pas ses communications écrites et ne les convoquerait pas aux débats. Indépendamment de leur participation active à la procédure ou non, toutes les parties plaignantes seraient toutefois servies d'une expédition du jugement de la Cour (SK 37.310.003 s.).

B.4.5 Dans le délai imparti pour ce faire, la partie plaignante B. a indiqué à la Cour souhaiter participer à la procédure et entendre prendre part aux débats (SK 37.551.038). La société C. a indiqué qu'elle souhaitait, elle, participer à la procédure mais renonçait à prendre part à l'audience (SK 37.552.032 s.). Les autres parties plaignantes n'ont pas donné de suite à l'interpellation du 17 décembre 2024.

La Cour a pris acte de ce qui précède par courrier du 21 janvier 2025 et dispensé de comparution aux débats les parties plaignantes qui ne souhaitaient pas y prendre part, soit toutes les parties plaignantes hormis B. (SK 37.310.006 s.). Elle a convoqué aux débats le représentant du MPC, le prévenu et son avocate Me Miriam Mazou ainsi qu'invité Me Sébastien Fanti à y participer, au nom de B.

(SK 37.331.001 ss et 37.351.001.004). La Cour a en outre délivré un sauf-conduit en faveur de A., conformément à sa requête (SK 37.400.021 s.).

B.4.6 Me Miriam Mazou a par la suite requis que A. soit dispensé de comparaître personnellement à la lecture du jugement, qui avait été agendée, dans l'intervalle, au 16 avril 2025. A l'appui de sa requête, la défense s'est prévalue du fait que le sauf-conduit que la Cour avait octroyé arrivait à échéance avant l'audience de lecture du jugement, que la présence du prévenu à celle-ci ne paraissait pas nécessaire et que Me Marie Besse, avocate en l'étude de Me Miriam Mazou, pouvait l'y représenter (SK 37.521.010). La Cour a communiqué aux parties que la requête de dispense du prévenu serait traitée aux débats (SK 37.400.059).

B.5 <u>De la réserve de la Cour quant à la qualification des faits</u>

B.5.1 Toujours dans le contexte de la préparation des débats, la Cour a préavisé les parties participant activement à la procédure qu'elle se réservait sa faculté d'examiner l'entier des faits décrits dans l'acte d'accusation à l'aune du chef d'utilisation frauduleuse d'un ordinateur au sens de l'art. 147 CP (art. 344 CPP), y compris sous l'angle de la tentative et du métier, par courrier du 11 mars 2025 (SK 37.400.043).

B.5.2 Par correspondance du 21 mars 2025, donnant suite à une demande du MPC, la Cour a encore précisé au sujet de sa réserve qu'à teneur des faits décrits dans l'acte d'accusation, l'accès indu aux données des sociétés lésées et la soustraction de celles-ci semblaient intrinsèquement liés aux détournements et tentatives de détournements de fonds commis au préjudice desdites sociétés et que, dans ces circonstances, tous les faits décrits par l'acte d'accusation pourraient relever de l'art. 147 al. 1 et 2 CP, à l'exclusion des art. 143 CP et 143bis CP. L'occasion serait donnée aux parties de se déterminer sur cette réserve aux débats (SK 37.400.051).

B.6 <u>De l'établissement des conditions de détention du prévenu</u>

B.6.1 Le 14 mars 2025, Me Miriam Mazou a demandé la production de rapports quant aux conditions de détention provisoire du prévenu auprès de la prison T. puis de la prison AA. (SK 37.521.007 s.).

B.6.2 La Cour a requis et obtenu des deux établissements carcéraux concernés des rapports circonstanciés (SK 37.262.1.001 ss et SK 37.262.2.001 ss).

B.6.3 Invitées par la Cour à se déterminer sur ces rapports de détention, les parties n'ont pas déposé d'observations à leur égard (SK 37.521.011 s.).

Il sera revenu sur les constations découlant desdits rapports ci-dessous (cf. ch. 7.7 *infra*).

C. Les débats

C.1 Les débats ont eu lieu le 7 avril 2025. Y ont comparu les représentants du MPC, soit le procureur fédéral Yves Nicolet et le procureur fédéral a.i. Jean-Philippe Peissard, le prévenu A. et ses défenseures, Me Miriam Mazou et Me Marie Besse (avocate en l'étude Mazou Avocats SA aux côtés de Me Miriam Mazou) ainsi que Me Sébastien Fanti, pour la partie plaignante B. Les autres parties plaignantes, dispensées de comparution, n'étaient pas présentes à l'audience (SK 37.720.003 s.).

C.2 Interpellées à l'ouverture des débats quant à leurs éventuelles questions préjudicielles, les parties n'en ont soulevé aucune (SK 37.720.004).

Les parties n'ont pas non plus apporté de remarque ou d'observation quant à la réserve de la Cour par rapport à la qualification juridique des faits (SK 37.720.005).

La Cour a ensuite procédé à l'audition du prévenu sur les faits et sa situation personnelle. Les parties présentes ont eu l'occasion de poser des questions complémentaires au prévenu (SK 37.731.001 ss).

Après avoir donné aux parties l'occasion de s'exprimer sur la demande de dispense de comparution du prévenu pour l'audience de lecture du jugement (cf. ch. B.4.6 *supra*) et aucune des parties présentes ne s'y opposant, la Cour a dispensé A. de comparution personnelle à ladite audience (SK 37.720.006).

Enfin, les parties ont été interpellées quant à leurs éventuelles réquisitions de preuve complémentaires, à l'issue de l'audition de A. par la Cour de céans. Les parties n'ont présenté aucune offre de preuve et la procédure probatoire a été close (SK 37.720.006 s.).

C.3 Il a ensuite été procédé aux réquisitoire et plaidoiries.

A l'issue de son réquisitoire, le MPC a pris les conclusions suivantes :

1. *Condamner A. à une peine privative de liberté de 36 (trente-six) mois de peine privative de liberté, dont 12 (douze) mois fermes, sous déduction de la détention provisoire déjà effectuée, et 24 mois avec sursis partiel pendant cinq ans ;*

2. *Prononcer à l'encontre de A. une créance compensatrice de CHF 500'000.- ;*

3. *Ordonner l'expulsion de A. du territoire suisse pour une durée de 5 ans ;*

4. *Mettre une part des frais de procédure, arrêtée à CHF 131'528.80, à la charge de A.*

C.4 Ensuite, Me Sébastien Fanti a plaidé au nom de B. et a conclu :

1. *A la condamnation de A. pour utilisation frauduleuse d'un ordinateur par métier (art. 147 al. 2 CP), tentative d'accès indu à un système informatique (art. 143bis CP), la condamnation pour escroquerie (art. 146 CP) étant laissée à l'appréciation de la Cour ;*

2. *A la condamnation de A. à une peine privative de liberté de 48 mois ;*

3. *A la condamnation de A. aux prétentions civiles de la société B. selon ses écritures du 5 juillet 2024 et sa liste de frais.*

C.5 Enfin, la défense a plaidé et pris les conclusions suivantes au nom de A. :

1. *Le libérer des chefs d'accusation de soustraction de données (art. 143 CP) et d'accès indu à un système informatique (art. 143bis CP).*

2. *Le libérer de tout chef d'accusation en lien avec les cas 1.3.2, 1.3.23, 1.3.24 et 1.3.25 de l'acte d'accusation.*

3. *Lui infliger, pour le surplus, une peine clémente compatible et assortie d'un sursis total.*

4. *Rejeter les conclusions civiles principales 3 et 4, de même que les conclusions subsidiaires 4 et 5, de la société B., ainsi que les conclusions civiles de la société J., subsidiairement renvoyer ces sociétés à agir par la voie civile.*

5. *Lui donner acte qu'il s'en remet à justice s'agissant des conclusions civiles des sociétés G. et C., ainsi que s'agissant de la conclusion principale 2 de la société B.*

6. *Renvoyer, pour le surplus, les parties plaignantes à agir par la voie civile.*

7. *Ordonner la libération de la caution de CHF 250'000.- déposée sur le compte du MPC auprès du Département fédéral des finances et le versement de ce montant sur le compte de consignation de l'Etude Mazou Avocats SA, dont les coordonnées sont les suivantes :*

   […]

8. *Lui allouer une indemnité pour l'exercice raisonnable de sa défense au sens de l'art. 429 CPP d'un montant d'à tout le moins CHF 31'325.-.*

9. *Mettre à sa charge une part équitable des frais de procédure, laquelle ne devra pas excéder CHF 65'764.40.*

10. *Constater l'irrecevabilité des conclusions de la partie plaignante B. s'agissant de la peine.*

C.6 Au terme des plaidoiries, l'occasion a été donnée à A. de s'exprimer une dernière fois (art. 347 al. 1 CPP). Le prévenu a fait usage de cette faculté en s'exprimant brièvement.

C.7 La lecture du jugement a eu lieu le 16 avril 2025, en présence des représentants du MPC et de Me Marie Besse, pour A. (SK 37.720.010). Ensuite, le dispositif du jugement du 16 avril 2025 a été notifié à toutes les parties.

Par courrier du 22 avril 2025, Me Miriam Mazou a déposé, au nom et pour le compte de A., une annonce d'appel (SK 37.940.001). Aucune des autres parties n'a annoncé appel dans le délai légal de 10 jours pour ce faire.

C.8 Par courrier du 9 mai 2025, Me Marc Bonnant a annoncé succéder à Me Miriam Mazou dans la défense des intérêts du prévenu (SK 37.521.013).

Faits

D. Implication de A. dans les fraudes

D.1 De l'implication reprochée à A.

D.1.1 Il est reproché à A. d'avoir, entre décembre 2016 et août 2018, à Netanya (IL) et en qualité de membre d'un groupe se livrant à des activités dites de *social engineering* (du type « arnaque au faux technicien bancaire »), contacté téléphoniquement diverses sociétés en Suisse, en se faisant passer pour un collaborateur de la banque de ces dernières, et d'avoir amené les employés responsables des paiements desdites sociétés à lui donner accès à leurs ordinateurs à leur insu et à ouvrir une ou plusieurs sessions *e-banking*, dans le dessein de permettre aux autres auteurs – qui n'ont pu être identifiés et ont fait l'objet d'une ordonnance de classement – de détourner des fonds. A. aurait ainsi accédé sans droit au système informatique de nombreuses sociétés et remis aux autres auteurs les données permettant d'y accéder, également sans droit, en sachant que ces données seraient utilisées dans le but de détourner des fonds. Il aurait en outre permis aux autres auteurs d'utiliser indument les données d'accès aux sessions *e-banking* pour ordonner le transfert d'importantes sommes d'argent par le débit des comptes des sociétés lésées en faveur de comptes en Suisse et à l'étranger, pour un montant total de CHF 5'309'036.20 (SK 37.100.003).

D.1.2 Selon l'acte d'accusation également, le mode opératoire utilisé par les auteurs était le suivant : après la collecte de renseignements sur une société susceptible de transférer des fonds à l'étranger, compilés sur une liste qui lui était remise, le prévenu prenait contact par téléphone avec un employé chargé des paiements de cette société en se faisant passer pour un représentant de la banque de cette dernière. Informant son interlocuteur qu'une modification du système *e-banking* (migration) devait avoir lieu sous peu et nécessitait des manipulations particulières chez les clients, le prévenu lui demandait d'ouvrir une ou plusieurs sessions *e-banking* et de la/les laisser ouverte(s) afin que la prétendue migration puisse avoir lieu. En parallèle, il demandait à l'employé d'introduire une adresse URL particulière dans la barre adresse de son navigateur internet, toujours au même prétexte. En réalité, l'adresse menait à un site permettant de télécharger des logiciels de contrôle à distance du type TeamViewer ou NTRCloud à l'insu de l'employé, et d'accéder ainsi directement à son ordinateur et, partant, au système informatique de la société visée. Une fois cet accès obtenu au moyen de l'intervention du prévenu, les autres auteurs utilisaient la session *e-banking* déjà ouverte, voire en ouvraient une eux-mêmes, puis ordonnaient indument le transfert d'importantes sommes d'argent par le débit des comptes de la société en faveur de comptes de tiers servant d'intermédiaires, en Suisse et à l'étranger (SK 37.100.004).

D.1.3 Ce faisant A. aurait en outre soustrait, à l'insu des sociétés lésées, leurs données d'accès ainsi que des informations concernant leurs comptes bancaires et leurs transactions financières, en accédant illicitement à l'ordinateur – et par la même aux sessions *e-banking* – des sociétés lésées (SK 37.100.004).

D.1.4 Par ces procédés, entre les mois de décembre 2016 et août 2018, le prévenu aurait apporté une contribution active et indispensable à des détournements de fonds au préjudice de sept sociétés sises sur le sol helvétique, ainsi qu'à de nombreuses autres tentatives de détournements (SK 37.100.004). Seule une partie des fonds soustraits ont pu être bloqués et retournés aux sociétés, le butin effectivement accaparé par les auteurs correspondant à environ CHF 5 millions, soit EUR 5'049'649.- ([EUR 307'078.- + EUR 1'905'102.- + EUR 274'193.- + EUR 772'098.- + CHF 722'151.- [correspondant à EUR 674'907.- au 24 janvier 2017, date de la transaction] + EUR 920'808.- + EUR 97'254.- + EUR 98'209.-] ; cf. ch. E.2.1, F.2.1, H.1.4 et H.2.1, J.1.4 et J.2.1, M.1.4, N.2.1 et O.2.1 *infra*). Au total, les fraudes reprochées au prévenu, dans l'acte d'accusation, visaient 25 sociétés différentes, ci-après désignées chacune comme un cas distinct – indépendamment du nombre de prises de contact téléphonique, de la réalisation de transferts de fonds et du nombre de ceux-ci.

D.2. Des aveux de A. quant à son implication

D.2.1 Dans un premier temps, A. a nié toute implication dans les faits sous enquête. Il a maintenu n'avoir aucun lien avec ceux-ci tout au long de ses auditions des 21 avril 2022 (MPC 13-01-0001 ss), 29 avril 2022 (MPC 13-01-0012 ss), 6 mai 2022 (MPC 13-01-0039 ss), 22 juin 2022 (MPC 13-01-0057 ss), 29 juin 2022 (MPC 13-01-0084 ss), 15 juillet 2022 (MPC 13-01-0168 ss) et 11 octobre 2022 (MPC 13-01-0184 ss).

D.2.2 Lors de son audition du 28 octobre 2022, le prévenu a déclaré vouloir s'expliquer (MPC 13-01-0235 ss). Il a alors, de manière générale, reconnu son implication dans l'activité frauduleuse en cause et a admis avoir participé à 13 des cas qui lui sont reprochés (MPC 13-01-0242 et 13-01-0247 ss). Il a aussi fourni des indications quant à son rôle et celui des autres personnes impliquées, leur mode opératoire et la clé de réparation du butin, tels que retenus, en substance, dans l'acte d'accusation (MPC 13-01-0236 ss). Lors d'une audition ultérieure, le 10 novembre 2022, le prévenu a admis un cas supplémentaire (cas C.), qu'il avait encore expressément nié le 28 octobre 2022 (MPC 10-05-0078) puis, dans un premier temps, le 10 novembre 2022 (MPC 13-01-0274). A. a expliqué qu'il n'avait jusqu'alors admis que les cas pour lesquels il avait bien perçu la part du butin lui revenant, ce qui n'était pas le cas s'agissant du détournement des fonds de C., dans lequel il avait toutefois été impliqué (MPC 13-01-0279 s.). Le prévenu a alors aussi admis, de manière générale, son implication dans diverses tentatives de fraude, effectuées sous les pseudonymes « BB. », « CC. » et « DD. » (MPC 13-01-0271). Enfin, pendant son audition du 30 novembre 2022, il a encore reconnu explicitement une série d'autres cas, dont sept lui sont reprochés dans l'acte d'accusation (MPC 13-01-0298).

Le prévenu a donc finalement admis 21 des 25 cas qui lui sont reprochés – en sus d'autres cas pour lesquels il a reconnu son implication mais qui ne lui sont pas reprochés selon l'acte d'accusation et dont la Cour de céans n'est dès lors pas saisie. Par-devant la Cour, A. a réitéré ses aveux s'agissant des 21 cas admis précédemment et a globalement confirmé les explications qu'il avait données en instruction (SK 37.731.014), qui sont en substance les suivantes :

D.2.3 A. a affirmé avoir toujours agi avec les trois mêmes autres individus, les dénommés « EE. » (que le prévenu appelle également « EE.a. » ou « EE.b. »), « FF. » et « GG. » (SK 37.731.010 et 37.731.014). Lui-même agissait en général sous les pseudonymes « BB. » et « CC. » (MPC 13-01-0258). Dans un premier temps, le prévenu a admis qu'il lui arrivait parfois d'utiliser d'autres pseudonymes, comme « DD. » (MPC 13-01-0266, 13-01-0271 et 13-01-298 s.) ou « HH. » (MPC 13-01-0273), avant de se rétracter lors d'interrogatoires ultérieurs (s'agissant de « HH. » : MPC 13-01-0299 ; s'agissant de « DD. » : SK 37.731.010). Par contre, le prévenu a, sans équivoque, affirmé et maintenu ne pas avoir utilisé les pseudonymes « II. » et « JJ. », respectivement

« KK. » (MPC 13-01-0274). Il expliqué que « FF. » et « EE. » avaient insisté pour qu'ils utilisent toujours les pseudonymes attribués (MPC 13-01-0258).

D.2.4 Toujours selon A., son rôle consistait à contacter téléphoniquement la société visée, en se faisant passer pour un collaborateur technique de la banque, et faire en sorte que son interlocuteur ouvre un lien – exécutant le programme de contrôle à distance – pour avoir accès à son ordinateur (MPC 13-01-0241 et SK 37.731.011). Le but de la démarche était de voir les identifiants et les accès au *e-banking*, sans que l'interlocuteur ne s'en aperçoive (MPC 13-01-0256). Pour ce faire, A. utilisait des informations sur la société, compilées sur une fiche (nom, adresse, numéro de téléphone, langue parlée, adresses e-mails, organigramme, chiffre d'affaires, secteur d'activité et existence d'une activité import-export) et, en général, préalablement vérifiées et complétées par des informations supplémentaires (nom de la banque de la société, celui du responsable des paiements au sein de la société et de la personne les validant et le mode d'utilisation *e-banking*), ce dont s'occupait, en principe, « GG. » (MPC 13-01-0269 et SK 37.731.010 s.). A l'aide de ces différentes informations, le prévenu essayait de comprendre le fonctionnement de la société (MPC 13-01-0256). Il effectuait ensuite son appel, lors duquel A. prétextait d'une migration informatique rendue nécessaire par le passage au virement SEPA et amenait son interlocuteur à se connecter à l'*e-banking* de la société et à ouvrir le raccourci URL exécutant le programme de contrôle à distance. Ce lien était préparé par « FF. », qui était assis aux côtés du prévenu pendant qu'il effectuait l'appel, et dicté par A. à son interlocuteur. Le lien permettait à A. et à « FF. » d'avoir ensemble un accès visuel à l'écran de l'ordinateur de la société, et parfois aussi à « FF. » de prendre les commandes de celui-ci. L'interlocuteur introduisait ses accès *e-banking* pour ouvrir la session, qui étaient alors visibles pour « FF. » et A., sur leur propre écran. « FF. » transmettait ensuite les accès *e-banking* de la société à « EE. », qui effectuait les transferts. Parfois, c'est « FF. » lui-même qui procédait aux transferts, depuis la session de la société. « FF. » et A. devaient alors rester en ligne – sur la session *e-banking* qui avait été ouverte par la société grâce aux manœuvres du prévenu – pendant que « FF. » opérait les transferts (MPC 13-01-0241, 13-01-0256 et 13-01-0269 ; SK 37.731.011 s.). Le prévenu et « FF. » devaient travailler en binôme pour pouvoir effectuer leur « travail » (MPC 13-01-0268), soit la deuxième phase de la fraude.

Il arrivait aussi parfois que A. collecte lui-même les informations sur les sociétés, soit qu'il effectue la tâche revenant (en principe) à « GG. » (MPC 13-01-0239, 13-01-0241, 13-01-0256, 13-01-0258 et SK 37.731.012). C'est d'ailleurs lui qui avait associé le dénommé « GG. » à l'activité frauduleuse en l'« engageant » pour établir les fiches (MPC 13-01-0240 et SK 37.731.012). A l'origine, « EE. » lui avait en effet expliqué que le travail d'appel devait être effectué par deux personnes puisqu'il y avait une première phase d'acquisition des informations sur l'entreprise, puis la seconde phase d'obtention des accès *e-banking* (MPC 13-01-0269).

Il est aussi arrivé au prévenu de modifier des relevés bancaires pour cacher les opérations de fraude (MPC 13-01-0241 et 13-01-0258).

D.2.5 S'agissant de sa manière de procéder lorsqu'il effectuait les appels, A. a expliqué qu'il amenait ses interlocuteurs à exécuter le programme de contrôle à distance en leur exposant qu'il était (soi-disant) nécessaire de vérifier quelle était leur version du programme *e-banking*, avant de débuter la migration informatique. Le prévenu leur laissait entrevoir que, faute de vérification (et de migration), les accès de la société à son *e-banking* pourraient être coupés (SK 37.731.013), donc qu'elle ne serait plus en mesure d'effectuer de paiements. A. disposait d'un argumentaire (« déballe »), que « FF. » lui avait fourni. Il disposait aussi d'un lexique de termes susceptibles d'être utilisés par son interlocuteur, afin de l'aider à comprendre de quoi ce dernier parlait. Pendant la conversation, le prévenu tapotait sur un clavier non-branché pour renforcer l'impression de son interlocuteur qu'il appelait depuis les bureaux de la banque (MPC 13-01-0255 s. et SK 37.731.012). Lors de ses appels, A. cherchait à susciter le trouble chez son interlocuteur, l'« embrouillait » (MPC 13-01-0257). Il demandait à ses interlocuteurs de ne pas se connecter à l'*e-banking* pendant la période de la soi-disant migration et s'assurait que les paiements en suspens aient été effectués avant le début de celle-ci. Ses manœuvres avaient pour but d'éviter que les collaborateurs de la société se connectent à l'*e-banking* et constatent les opérations de débit sur les comptes (SK 37.731.013). La démarche tendait ainsi à éviter que les lésés se rendent compte à temps des débits frauduleux et puissent entreprendre des démarches pour bloquer les transactions ou rapatrier leurs fonds (SK 37.731.014).

Comme cela ressort de certains enregistrements des appels de A., il arrivait que le prévenu pose à ses interlocuteurs des questions quant aux habitudes de paiement de la société (cf. ch. E.2.2. s., P.2.3, R.2.3 et S.2.3 *infra*). Il a affirmé que la collecte de telles informations faisait partie de la première phase de la fraude, soit celle effectuée (en principe) par « GG. ». Ces informations-ci avaient pour objectif de conformer le montant et la destination des transactions frauduleuses aux habitudes de paiement de la société, aux fins d'éviter que ces paiements frauduleux soient découverts par la banque. « EE. » était présent, « à côté », pendant la collecte desdites informations, en disposait donc, et les utilisait pour effectuer les versements (SK 37.731.012).

D.2.6 S'agissant du butin, A. a expliqué que celui-ci était réparti et qu'une part de 45% des montants détournés revenait à « EE. », « FF. », « GG. » et lui-même, qui se répartissaient cette part entre eux à raison de 60% pour « EE. » et « FF. » et 40% pour le prévenu et « GG. ». Le solde du butin (55%) rémunérait les titulaires des différents comptes utilisés pour faire transiter l'argent (45%) ainsi que d'autres personnes en Israël (10%) (MPC 13-01-0240, SK 37.731.016 et 37.731.019).

La rémunération supérieure de « FF. » et « EE. » (60%) par rapport à la part revenant au prévenu et « GG. » (40%), visait à rétribuer la mise à disposition de l'infrastructure par les premiers (MPC 13-01-0240).

A. partageait équitablement avec « GG. » la part qui leur revenait (MPC 13-01-0242). Il a ainsi perçu 9% du butin (0.4 x 0.45/2), part qu'il a désignée en procédure comme étant sa « commission ».

Dès qu'un virement était effectué, « FF. » informait A. qui prenait ces informations et les notait sur une feuille (MPC 13-01-0276). Le prévenu touchait sa « commission » environ une semaine après chaque détournement de fonds, à Tel-Aviv (IL). La « commission » lui était remise en liquide, par « EE. » (MPC 13-01-0242, 13-01-0244 et 13-01-0276), avec celle revenant à « GG. ». C'est le prévenu qui remettait celle-ci à « GG. » (MPC 13-01-0276).

En sus, de sa « commission », le prévenu percevait une rétribution fixe de EUR 6'000.- par mois d'activité, son « salaire » (MPC 13-01-0240 et SK 37.731.020).

A. n'a pas tenu de décompte de ses commissions (MPC 13-01-0276 et SK 37.731.017). Selon ses déclarations, il aurait perçu au maximum EUR 200'000.- pour ses activités délictueuses, puis versé 10% de ce montant à des œuvres de charité et dépensé intégralement le reste des fonds pour des voyages et des habits (MPC 13-01-0244 et SK 37.731.018). Il estime toutefois n'avoir pas toujours reçu la « commission » qui lui était due. Le prévenu avait en effet constaté qu'il y avait parfois des petites différences entre le montant prévisible de sa « commission » et le montant effectivement remis par « FF. ». Il l'avait constaté, au moment de faire les comptes avec « EE. », grâce aux informations qu'il recevait de « FF. » quant aux montants des transferts, à chaque virement (MPC 13-01-0276 et SK 37.731.018). « EE. » lui donnait alors des excuses pour expliquer la différence entre la commission attendue par le prévenu et celle qui lui avait été effectivement remise (MPC 13-01-0259, 13-01-0276 et SK 37.731.019). A. a estimé que « GG. » et lui s'étaient « fait voler » une partie de leur « commission » par « FF. » et « EE. » (SK 37.731.019).

D.2.7 Quant à ses motivations et sa prise de contact avec ses acolytes, A. a expliqué avoir fait la connaissance de « EE. » en boîte de nuit, en décembre 2016. Le premier avait parlé au second de ses activités professionnelles en tant que DJ, dans les assurances et dans le *lead marketing* (consistant à établir et vendre des listes de clients commerciaux potentiels ; MPC 13-01-0005) ainsi que du fait qu'il cherchait un nouvel emploi, éprouvant sa situation financière comme difficile. « EE. » lui avait parlé de son activité de « décaisse », que le prévenu savait être un processus consistant « à recevoir et à faire sortir de l'argent par des comptes bancaires mis à disposition par des intermédiaires » et qu'il estimait similaire au blanchiment d'argent en matière de stupéfiants. « EE. » lui avait proposé de

travailler avec lui, précisant que l'activité n'était pas « propre » mais qu'elle permettait de gagner rapidement beaucoup d'argent, soit de EUR 10'000.- à EUR 50'000.- par opération. D'une part, A. avait ressenti de la jalousie, car « EE. » gagnait bien sa vie. Le prévenu avait été tenté, ayant vécu la situation financière difficile de ses parents et s'étant promis de ne jamais faire vivre une situation similaire à ses propres enfants (MPC 13-01-0238). D'autre part, il avait aussi ressenti des scrupules à accepter la proposition de « EE. », notamment en raison de ses convictions religieuses et de ses valeurs morales (MPC 13-01-0236 s.). L'appât du gain avait finalement pris le dessus et, après réflexions, le prévenu avait recontacté « EE. », au début décembre 2016, pour lui signaler son intérêt.

Lors de l'entrevue qui s'en était suivie, « EE. » lui avait expliqué le fonctionnement des fraudes et lui avait demandé de trouver quelqu'un pour effectuer la première étape de celle-ci, soit la collecte d'informations sur les sociétés. « EE. » avait précisé d'entrée de cause qu'il travaillait avec des voyous mais que le prévenu n'aurait pas besoin de les rencontrer (MPC 13-01-0238 s.). A. avait alors négocié ses conditions, demandant à recevoir un « salaire » fixe de EUR 5'000.- à EUR 6'000.-, parce qu'il avait charge de famille. Il a alors aussi été convenu qu'il reçoive, en sus de ce « salaire », sa « commission » et A. s'est renseigné auprès de « EE. » au sujet de la clé de répartition du butin (MPC 13-01-0240).

Le jour même, le prévenu avait engagé « GG. » et, dès le lendemain, ils avaient rencontré ensemble « FF. » qui avait expliqué ses tâches à « GG. ». Pour A., les choses étaient un peu plus compliquées que pour « GG. ». Il était en effet important que le discours de A. paraisse naturel et professionnel, et qu'il agisse de manière coordonnée avec « FF. ». Ce dernier lui avait expliqué comment procéder puis ils avaient fait des simulations lors desquelles le prévenu devait s'adapter aux aspects techniques permettant de se connecter au poste de la société visée, sur la base des liens que « FF. » créait pour pouvoir obtenir un accès à distance au poste. Ils s'étaient ainsi entraînés plusieurs jours jusqu'à obtenir un rythme de croisière et des automatismes avant de « travailler », c'est-à-dire d'effectuer les appels aux sociétés (MPC 13-01-0241 et 13-01-0256).

D.2.8 S'agissant enfin de sa période d'activité dans les fraudes, A. a d'abord indiqué avoir débuté celle-ci en décembre 2016 et y avoir mis un terme provisoire après son engagement auprès de la société 11, à Netanya (IL), intervenue le 1er novembre 2017 (MPC 13-01-0270). Il avait ensuite repris les fraudes au mois de juin (*recte* : mai) 2018 (MPC 13-01-0243). Par la suite, le prévenu a relativisé ses indications et a admis avoir poursuivi ses agissements, au-delà de sa prise de service auprès de la société 11, et avoir bien continué à participer à des fraudes aux mois de novembre et décembre 2017 (id. et MPC 13-01-0302).

D.3 Des cas pour lesquels A. nie toute implication

D.3.1 A. reconnaît son implication susdécrite pour 21 des cas qui lui sont reprochés mais la nie pour quatre d'entre eux, à savoir ceux relatifs à F. (chiffre 1.3.2 de l'acte d'accusation), à la société 9, aujourd'hui société 9.a. (chiffre 1.3.24 de l'acte d'accusation), J. (chiffre 1.3.23 de l'acte d'accusation) et Q. (chiffre 1.3.25 de l'acte d'accusation).

D.3.2 Le prévenu fait aussi valoir n'avoir pas perçu plus de EUR 200'000.- au total pour les fraudes, sans toutefois être en mesure de préciser si ce montant correspondrait à la seule part « commission » ou également à la part « salaire » (SK 37.731.016).

D.4 Il sera revenu ci-après sur chacun des cas reprochés au prévenu conformément à l'acte d'accusation.

E. Cas G. (anc. G.a. et G.b.) (chiffre 1.3.1 de l'acte d'accusation)

E.1 Des faits reprochés au prévenu

E.1.1 A teneur de l'acte d'accusation, le 22 décembre 2016, vers 10h45, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a appelé la société G.a. à U. (aujourd'hui : G.). Se présentant sous l'identité de « BB.a. », employé de la banque 4, le prévenu s'est entretenu avec LL., assistante-comptable de cette entreprise, à laquelle il a expliqué qu'une migration du système *e-banking* devait avoir lieu.

E.1.2 Après lui avoir posé diverses questions sur les habitudes de paiement de l'entreprise, le prévenu a prié LL. d'introduire dans la barre adresse de son navigateur internet l'adresse URL « www.1 » suivie d'un numéro qu'il lui a communiqué. Cette adresse était en réalité un lien raccourci cachant l'adresse réelle à laquelle il renvoyait, soit celle du site « www.2 » offrant un service de contrôle à distance. Le prévenu a ainsi amené son interlocutrice à télécharger à son insu le logiciel de contrôle à distance NTRCloud qui lui a permis d'accéder indument à l'ordinateur de l'assistante-comptable et, partant, aux serveurs de la société susmentionnée.

E.1.3 Le prévenu a ensuite demandé à son interlocutrice d'ouvrir une session *e-banking* sur les comptes de la société et, une fois la session ouverte, lui a posé des questions relatives au paiement des fournisseurs et la devise utilisée pour ceux-ci, avant de la prier de quitter la session. Le prévenu a alors insisté pour que LL. vérifie les accès à l'*e-banking* de l'administrateur de la société, NN. Ce dernier a remis ses codes d'accès et sa calculette – soit l'appareil nécessaire à la génération du code d'accès de validation pour ouvrir la session *e-banking* – à LL. qui a ainsi pu répondre aux questions du prévenu sur les paiements à

effectuer d'ici au lendemain soir. Au moyen de l'accès à l'ordinateur de l'assistante-comptable, le prévenu a pu prendre connaissance sans droit des données bancaires de la société.

E.1.4 Le même jour vers 16h, le prévenu a rappelé LL. et l'a priée à nouveau d'introduire dans son navigateur l'adresse URL « www.1 », lui permettant ainsi d'accéder indument à son ordinateur. Il lui a ensuite demandé d'ouvrir une session *e-banking*. La précitée s'est exécutée en utilisant le numéro de contrat du responsable financier de la société, OO. Après avoir communiqué les codes générés par la calculette de la banque au prévenu à sa demande, LL. s'est déconnectée. Le prévenu lui a alors demandé de se connecter au moyen des accès de NN., lequel avait communiqué ceux-ci à l'assistante-comptable. Cette dernière lui ayant signifié qu'elle devait encore saisir des paiements dans le système *e-banking*, elle a convenu avec le prévenu qu'il la rappellerait le lendemain entre 9 et 10h. Avant de se déconnecter, et à la demande du prévenu, elle lui a communiqué tous les codes d'accès, qu'il a à son tour remis aux autres auteurs afin qu'ils puissent eux-mêmes les utiliser pour ouvrir une ou plusieurs sessions *e-banking*.

E.1.5 Le lendemain, soit le vendredi 23 décembre 2016, après un premier entretien téléphonique entre 9 et 10h, LL. a rappelé le prévenu en lui indiquant que tous les paiements avaient été saisis. Les autres auteurs ont alors utilisé les accès au système *e-banking* communiqués par le prévenu dans le but de générer un code préalable à l'ouverture d'une session. Le prévenu a ensuite prié LL. d'introduire dans la calculette de la banque les codes que les autres auteurs avaient générés par l'introduction des numéros de contrat d'OO. puis de NN. dans les sessions *e-banking* et de lui communiquer les codes en résultant. Une fois en possession de ces codes, le prévenu les a remis aux autres auteurs qui ont pu finaliser l'ouverture de la session *e-banking* sur les comptes de la société. Il a encore discuté avec son interlocutrice puis lui a indiqué qu'il ne fallait plus effectuer aucune opération dans l'*e-banking* durant la migration, la priant également de prendre les calculettes afin d'éviter que les titulaires des comptes ne se connectent. Il a encore annoncé qu'il rappellerait la société le lundi 9 janvier 2017.

E.1.6 Le 23 décembre 2016, entre 11h50 et 12h, depuis un endroit non déterminé en Israël, au moyen des accès *e-banking* ainsi obtenus par le prévenu, les autres auteurs ont pris connaissance sans droit des données bancaires de la société. Ils ont en outre pu ordonner indument les deux transferts suivants, à l'insu des responsables des sociétés, par le débit du compte 10 (EUR) de la banque 4 au nom de la société :

1) EUR 97'257.- en faveur de la société 12, sise […] à Dortmund (D), sur le compte 11 auprès de la banque 5 à Francfort-sur-le-Main (D) ;

2) EUR 209'821.- en faveur de la société 13, à Amstelveen (NL), sur le compte 12 auprès de la banque 6 à Amsterdam (NL).

E.1.7 Le même jour, les auteurs ont encore tenté de transférer indument un montant de USD 395'971.- par le débit du compte de la banque 4 susmentionné en faveur de la société 14 en Chine. Ce transfert a toutefois été bloqué par la banque 4.

E.1.8 Ainsi, le préjudice subi par la partie plaignante s'élève à EUR 307'078.- (EUR 97'257.- + EUR 209'821.-).

E.2 Des moyens de preuve

E.2.1 A l'appui de sa plainte pénale, la société a produit les détails de transactions (avis de débit et swifts) de la banque 4, dont il ressort que le compte lié au numéro IBAN n° 10 de la relation bancaire au nom de G.a. a bien été débité, par ordre global *e-banking* daté et exécuté le 23 décembre 2016, d'un montant total de EUR 307'078.-. Ce montant correspond à deux transactions, l'une en faveur de la société 13, […], Amstelveen (NL), par EUR 209'821.-, et l'autre en faveur de la société 12, […], Dortmund (D) (MPC 05-12-00040 à 05-12-0042). La transaction d'USD 395'971.00 en faveur de la société 14 a, elle, été bloquée par la banque de la société bénéficiaire (MPC 05-12-0039 et 05-12-0041).

E.2.2 L'enquête a en outre permis de saisir un enregistrement audio de l'entretien téléphonique du 9 janvier 2017 entre LL. et « M. BB. », puis « M. BB. » et OO. (annexe au rapport PJF du 30 mars 2023). Au cours de celui-ci, « M. BB. » demande à LL. d'ouvrir le « SEPA guide » et lui demande de se connecter à « www.36 ». Il s'enquiert en outre de la date des prochains versements et du type de saisie, DTA ou manuelle, ainsi que du type de destinataires des versements (salaire ou fournisseur). OO. confronte ensuite « M. BB. » aux trois débits frauduleux, soit un en dollars et deux en euros, ce sur quoi « M. BB. » affirme qu'il s'agirait de débits fictifs, prétextant que la société devrait, normalement, déjà avoir récupéré les montants en cause. « M. BB. » passe alors en revue les montants, prétendant que le versement d'environ EUR 97'000.- devrait être crédité le lendemain sur le compte de la société. OO. insistant pour obtenir des informations, « M. BB. » change de sujet et demande à savoir qui s'est connecté à l'*e-banking*, puis reproche à OO. de n'avoir pas suivi ses instructions contraires. « M. BB. » prétend encore que la situation est normale et que la migration ne serait pas encore terminée, raison pour laquelle, à première connexion, OO. ne verrait pas encore les montants (fictivement) débités. Lorsqu'OO. lui indique que la banque l'a informé d'un découvert, « M. BB. » lui annonce que la banque va lui transmettre un e-mail de confirmation pour le rassurer.

E.2.3 Entendue le 9 janvier 2017 (MPC 05-12-0027 ss), LL. a décrit la prise de contact de « M. BB. », telle que reprochée au prévenu dans l'acte d'accusation. Elle a ainsi, en substance, expliqué que « M. BB. », se présentant comme un

collaborateur de la banque 4, l'a contactée le 22 décembre 2016, vers 10h45. Il lui a alors expliqué que la banque allait faire une migration du système *e-banking* et que selon la version internet dont disposait l'entreprise, cela pouvait engendrer des problèmes et prendre du temps. « M. BB. » l'a encore questionnée sur les habitudes de paiement de l'entreprise. Ensuite, « M. BB. » a demandé à LL. de se connecter sur internet, d'introduire l'URL 1 et de cliquer sur le bouton « exécuter ». Toujours sur instruction de « M. BB. », LL. s'est alors connectée à l'*e-banking* de la société, avec le contrat d'OO. A la demande de « M. BB. », elle a ensuite essayé d'effectuer le même processus avec les accès de NN., sans succès. Finalement « M. BB. » l'avait recontactée vers 16h00 le même jour et l'a accompagnée à travers les mêmes étapes de connexion, d'abord avec le contrat *e-banking* d'OO., puis avec celui de NN. « M. BB. » lui a alors signifié souhaiter débuter la migration, sur quoi LL. l'a informé que cela n'était pas possible, dès lors qu'elle devait encore saisir des paiements. Le lendemain matin, « M. BB. » a une fois de plus recontacté LL. pour s'assurer que les paiements avaient été saisis et l'a intimée de ne pas se connecter à l'*e-banking* pendant toute la durée de la migration, qui allait débuter.

E.2.4 Entendu le 10 janvier 2017, OO. a précisé que les paiements *e-banking*, préparés par LL. à l'aide des codes d'accès d'OO., doivent être validés par NN. (MPC 05-12-0034), une double signature étant nécessaire pour effectuer les transactions.

E.2.5 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier le détournement de fonds au préjudice de la société G.a., aujourd'hui G. (MPC 13-01-0091 et 13-01-0194), y compris lorsque confronté à l'enregistrement audio susmentionné, prétendant ne pas reconnaître les voix sur celui-ci (MPC 13-01-0091 et 13-01-0171). Lors de son audition du 28 octobre 2022, le prévenu a finalement admis être « M. BB. » qui avait contacté la société (MPC 13-01-0241 et 13-01-0247 ss). Il a aussi affirmé se souvenir qu'il s'agissait de la première société qu'il avait contactée, précisément parce que la raison sociale de la société comportait le nom de famille « BB. », soit son pseudonyme (MPC 13-01-0241 et 13-01-0273).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

F. F. (chiffre 1.3.2 de l'acte d'accusation)

F.1 <u>Des faits reprochés au prévenu</u>

F.1.1 A teneur de l'acte d'accusation, à une date indéterminée située entre le 19 et le 22 décembre 2016, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a appelé F. à Genève en se présentant sous le nom de « HH.a. », prétendument employé par la banque 4. Le prévenu a indiqué à son

interlocuteur MM. que la banque précitée allait procéder à une « migration » de la plateforme de paiement afin d'améliorer son accessibilité et d'éliminer des problèmes de lenteurs constatés.

F.1.2 Le 22 décembre 2016, le prévenu a rappelé MM. en lui proposant d'entamer ladite migration. Lors du même appel, le prévenu s'est également entretenu avec un autre employé de F., à savoir PP., lequel lui a indiqué que les paiements de la société seraient finalisés à 16h.

F.1.3 Le même jour, à 16h45, le prévenu a rappelé MM. Sous le prétexte de démarrer la prétendue migration de la plateforme de paiement, il a convaincu son interlocuteur d'entrer dans la barre adresse de son navigateur une adresse URL communiquée oralement, l'amenant ainsi à télécharger à son insu le logiciel de contrôle à distance DDDD. et à lui permettre d'accéder de la sorte indument à son ordinateur et, partant, aux serveurs de la société susmentionnée. Cet accès obtenu, le prévenu a prié MM. et PP. de se connecter à leurs sessions *e-banking* respectives sur le poste informatique du premier nommé. Une fois les sessions ouvertes, et au moyen de la connexion à distance, le prévenu a pris connaissance sans droit des données d'accès au compte *e-banking* de F., ainsi que des données bancaires de celle-ci. Il a alors communiqué les accès à l'ordinateur de MM. et aux sessions *e-banking* précitées aux autres auteurs, en sachant que ces derniers les utiliseraient pour ordonner des transferts indus au préjudice de la société précitée.

F.1.4 Toujours le même jour, depuis un endroit non identifié en Israël et au moyen des accès ainsi obtenus par l'intervention du prévenu, les autres auteurs ont pu ordonner le transfert indu de EUR 992'728.- (CHF 1'067'754.41) par le débit du compte 13 au nom de F. auprès de la banque 4 en faveur du compte bancaire n° 14 ouvert au nom de la société 15 auprès de la banque 7.

F.1.5 Le 28 décembre 2016, le prévenu, toujours sous la fausse identité de « HH.a. », s'est à nouveau entretenu avec MM. au sujet de paiements qui devaient être effectués par le système *e-banking*. Il a été convenu que lesdits paiements seraient passés le lendemain. Le 29 décembre 2016, le prévenu a derechef contacté MM. puis, sous le prétexte fallacieux de l'assister dans le processus de paiements en cours, s'est indument connecté à distance sur son poste. Il a ensuite prié le précité et QQ., également employé de F., d'ouvrir une session *e-banking* pour lui permettre de valider les paiements. Le prévenu a ensuite remis les accès directs au poste de MM. aux autres auteurs qui ont pu cette fois transférer sans droit le montant de EUR 912'374.- (CHF 985'253.52) par le débit du compte 13 au nom de F. auprès de la banque 4 en faveur du compte bancaire n° 14 ouvert au nom de la société 15 auprès de la banque 7.

F.1.6 Le préjudice subi par la plaignante s'élève ainsi à CHF 2'053'007.93 (CHF 1'067'754.41 + CHF 985'263.52 [correspondant aux deux transferts de EUR 992'728.- et EUR 912'374.-, soit EUR 1'905'102.-]).

F.2 Des moyens de preuve

F.2.1 A l'appui de sa plainte du 9 janvier 2017, F. a produit les détails de transaction (avis de débit et extrait swift) pour les deux transactions en cause. Il en ressort qu'un premier montant de CHF 1'067'754.41 a été débité de la relation bancaire de F. sur ordre *e-banking* du 23 décembre 2016, correspondant au versement de EUR 992'728.- en faveur de la société 15 (MPC 05-02-0027 et 05-02-0278) et qu'un second débit, par CHF 985'253.52, a été opéré par ordre *e-banking* du 30 décembre 2016, correspondant, lui, au versement de EUR 912'374.- en faveur de la même société (MPC 05-02-0028 et 05-02-0281).

F.2.2 Par ailleurs, il ressort de la documentation bancaire du compte de la société 15 auprès de la banque 7 que celle-ci a été créditée des deux versements en cause (MPC 05-02-193 s. et 05-02-00197 s.).

F.2.3 Le déroulement des faits reprochés au prévenu est corroboré par la plainte déposée par F. le 9 janvier 2017 (MPC 05-02-0016 ss). A teneur de ladite plainte, la première prise de contact de « HH.a. » est intervenue dans la semaine du 19 décembre 2016, à une date qui n'a pas pu être précisée plus avant (MPC 05-02-0019). On relèvera encore que, toujours selon la plainte du 9 janvier 2017, le prétendu « HH.a. » a communiqué à MM. deux numéros de téléphone pour le rappeler, soit le 15 et le 16, le 22 décembre 2016 à 10h23 (MPC 05-02-0019).

Or, le numéro de téléphone 15 est un des deux raccordements utilisés par « BB.a. » pour appeler son interlocutrice auprès de la société G.a., aujourd'hui G., à cinq reprises, entre le 22 et le 23 décembre 2016 (MPC 05-12-0029). Le numéro 16 est celui sur lequel elle devait rappeler « BB.a. », le 9 janvier 2017 (MPC 05-12-0029). Il s'agit du même numéro que celui indiqué dans l'e-mail de « BB.a. » du 4 janvier 2017 à l'attention de I. (MPC 05-02-0047) ou de celui signé « HH.a. » du 9 janvier 2017 adressé à la société K. (MPC 05-02-0057). C'est aussi ce raccordement que « BB. » a indiqué être son numéro à son interlocutrice auprès de la société H., le 4 janvier 2017 (MPC 05-05-0030). A. a reconnu avoir exécuté les cas G.a. (aujourd'hui G.), I., K. et H.

A. a expliqué avoir utilisé deux téléphones portables pour contacter les sociétés lésées, lesquels restaient posés sur son bureau pour l'éventualité où l'employé de la société rappellerait. Tant « GG. », « FF. » que le prévenu répondaient aux appels entrants (MPC 13-01-0255 et 13-01-0257). Les raccordements étaient chacun utilisés pendant une semaine, soit un, deux ou trois cas (MPC 13-01-0306). S'agissant du courriel signé « HH.a. », envoyé à K., il a indiqué en

instruction qu'il s'agissait d'une erreur de « FF. » et que lui (le prévenu) aurait fait attention à ne pas signer « HH.a. » (MPC 13-01-0307).

F.2.4 Le prévenu nie toute implication dans le détournement des fonds de F. En premier lieu, il se prévaut du fait que la prise de contact avec ladite société serait, selon lui, antérieure à celle avec G.a., aujourd'hui G., qu'il se souvient avoir été la première société qu'il ait contactée (MPC 13-01-0273 et SK 37.731.015). Deuxièmement, le prévenu indique ne pas se souvenir d'avoir touché une « commission » correspondant aux montants détournés du compte de F. et que – eu égard au montant détourné – s'il avait touché une telle « commission », il s'en souviendrait (MPC 13-01-0273). Troisièmement, le prévenu a indiqué n'avoir que peu utilisé le pseudonyme « HH. » (MPC 13-01-0273). Ultérieurement, il a affirmé ne l'avoir, en fait, jamais utilisé (MPC 13-01-0299 et 13-01-0307).

La Cour relève que A. a indiqué penser avoir lui-même effectué la première phase de collecte d'informations dans le cas G., avant d'effectuer la deuxième phase d'obtention des accès *e-banking* (MPC 13-01-258) et qu'il avait été en contact avec ladite société à plusieurs reprises, jusqu'au début janvier 2017. Elle relève aussi que les fraudes ont été perpétrées, pour partie du moins, en parallèle, comme cela ressort du relevé des appels (13-01-0293 ss). Par ailleurs, la Cour constate que le prévenu s'est prévalu de n'avoir pas perçu de « commission » correspondant au montant détourné non seulement dans le cas F. mais aussi dans celui de C., pour en déduire n'avoir pas été impliqué dans ces cas (MPC 13-01-247, 13-01-0273 s. et 13-01-0275). Par la suite, il a fini par admettre qu'il avait, en fait, bien participé à la réalisation du cas C. (MPC 13-01-0279) et a expliqué avoir jusqu'alors maintenu ses dénégations parce qu'il n'avait pas touché de « commission » en raison de soi-disant problèmes avec un compte, ce qui avait donné lieu à un différend avec « EE. » (MPC 13-01-0279 et 13-01-0299 s.).

Lors des débats par-devant la Cour de céans, bien que confronté au fait que l'obtention des accès *e-banking* de F. avait peut-être eu lieu après l'appel à G.a., aujourd'hui G., le prévenu a maintenu ses dénégations, au motif que la première société qu'il avait contactée avait été la société G. Il a affirmé que c'étaient sûrement « EE. » et « FF. » les auteurs de l'appel à F. (SK 37.731.015). Il a toutefois aussi exclu que ces derniers utilisaient le pseudonyme « HH. » (SK 37.731.011).

G. I. (chiffre 1.3.3 de l'acte d'accusation)

G.1 Des faits reprochés au prévenu

G.1.1 A teneur de l'acte d'accusation, le 4 janvier 2017, vers 10h30, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté téléphoniquement la société I. à V. Se présentant auprès de la comptable RR. sous la fausse identité de « BB.a. », il a affirmé à son interlocutrice qu'il représentait la banque 4, laquelle effectuait des modifications de son système *e-banking*, et qu'il voulait s'assurer que le programme informatique de I. supportait ces modifications. Il a alors amené RR. à télécharger à son insu le logiciel d'accès à distance NTRCloud en lui dictant une adresse URL, à savoir « 3 ». Le prévenu a ainsi pu accéder indument à l'ordinateur de RR. et, partant, aux serveurs de I. et, par la même, prendre connaissance de données de la société précitée, en particulier les données d'accès de RR. Il a de la sorte pu fournir à celle-ci le code généré par la plateforme *e-banking* de la banque 4 grâce à ces données d'accès, puis a prié la comptable d'introduire ledit code dans la calculette de la banque 4, permettant à RR. d'ouvrir une session. Le prévenu a communiqué ces données d'accès et l'accès lui-même aux autres auteurs dans le but de leur permettre d'ordonner des transferts indus au préjudice de I.

G.1.2 RR. s'est ensuite déconnectée de cette session *e-banking* et elle a refusé de se reconnecter au moyen de la carte d'une de ses collègues comme le prévenu le lui demandait. En raison des soupçons que la conversation susmentionnée lui avait inspirés, elle a appelé la véritable banque 4 et a fait bloquer le compte de la société.

G.1.3 Le 6 janvier 2017, le prévenu a rappelé la société I. et a à nouveau tenté de faire télécharger le logiciel NTRCloud à son interlocuteur, sans succès toutefois, l'informaticien de la société ayant assisté à la manœuvre.

G.1.4 Aucun détournement n'a pu être commis par les auteurs sur ce compte.

G.2 Des moyens de preuve

G.2.1 A l'appui de sa plainte du 5 janvier 2017, I. a notamment produit la copie des courriels que « BB.a. » lui avait adressés (MPC 05-02-0038 ss) ainsi qu'un relevé des deux appels effectués depuis le numéro 17, le 4 janvier 2017 (MPC 05-002-0041).

G.2.2 Le déroulement des événements reprochés au prévenu est corroboré par la plainte pénale et les déclarations de RR. du 5 janvier 2017 (MPC 05-02-0030 ss). En substance, celle-ci a expliqué que « BB.a. » de la banque 4 l'avait contactée le 4 janvier 2017 vers 10h30, lui expliquant que la banque procédait à des modifications sur son portail *e-banking*. A cet effet, il voulait s'assurer de la compatibilité du programme de I. RR. a encore demandé à « BB.a. » une preuve

qu'il était bien employé de la banque et elle a alors reçu un courriel en provenance d'une adresse e-mail de celle-ci et comportant son logo, ce qui l'a mise en confiance. « BB.a. » l'a ensuite accompagnée à travers diverses manipulations sur le portail *e-banking*. Il a ensuite demandé à RR. de répéter ces opérations avec les accès de sa collègue, ce que RR. a refusé (MPC 05-02-0031).

G.2.3 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier la prise de contact avec la société I. (MPC 13-01-0091). Lors de son audition du 28 octobre 2022, le prévenu a finalement admis être « BB.a. » qui avait contacté I. (MPC 13-01-0247 ss).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

H. H. (chiffre 1.3.4 de l'acte d'accusation)

H.1 Des faits reprochés au prévenu

H.1.1 A teneur de l'acte d'accusation, le mercredi 4 janvier 2017, entre 15h et 16h, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a appelé téléphoniquement la société H. à W. Il s'est présenté sous l'identité de « M. BB. », prétendument employé de la banque 4, plus précisément du Customer Service de cette banque, auprès de la responsable des finances, SS., à qui il a expliqué qu'il devait procéder à une mise à jour du logiciel *e-banking* de la société. Le prévenu a ensuite prié son interlocutrice d'entrer l'adresse suivante sur son navigateur Internet : « http://4 », au moyen de laquelle il l'a amenée à télécharger le logiciel de contrôle à distance NTRCloud sur son PC. Il a ensuite communiqué un identifiant à SS. qui lui a alors remis le code à 8 chiffres généré par le logiciel, que le prévenu a utilisé pour se connecter sans droit à distance sur l'ordinateur de son interlocutrice.

H.1.2 A la demande du prévenu, la responsable des finances de H. s'est ensuite connectée à une session *e-banking* liée aux comptes de l'entreprise. Grâce au logiciel de contrôle à distance susmentionné, le prévenu a alors amené la lésée à masquer son propre écran, en appuyant sur la touche F5, lui permettant ainsi de prendre connaissance à son insu des données bancaires de la société dans le cadre de la session *e-banking* qui était ouverte. Comme SS. devait encore effectuer des paiements pour la société, le prévenu lui a proposé de les examiner avec elle sur une autre session *e-banking*. A la demande de SS., le prévenu lui a ensuite communiqué une confirmation des paiements de l'entreprise qu'il avait lui-même réglés par *e-banking*.

H.1.3 Grâce au logiciel de contrôle susmentionné, le prévenu a ainsi indument accédé à l'ordinateur de SS. et, partant, au système informatique de la société susmentionnée. Il a en outre pris ainsi connaissance sans droit des données bancaires de la société H. Il a également communiqué les données d'accès à l'*e-banking* et l'accès à l'ordinateur de SS. aux autres auteurs. Ceux-ci ont ainsi pu, depuis un endroit en Israël qui n'a pu être déterminé précisément, ouvrir des sessions *e-banking* directement sur l'ordinateur de SS., prendre connaissance à leur tour des données bancaires de la société et ordonner les 6 transferts de fonds suivants par le débit du compte n° 18 au nom de H. auprès de la banque 4 :

1) le 5 janvier 2017, EUR 297'157.- en faveur du compte n° 19 au nom de la société 16 auprès de la banque 7 ; ces fonds ont été recrédités sur le compte de la lésée ;

2) le 5 janvier 2017, EUR 143'147.- en faveur du compte 20 au nom de la société 12.a. auprès de la banque 5 à Francfort-sur-le-Main (D) ; ces fonds ont été recrédités sur le compte de la lésée ;

3) le 9 janvier 2017, EUR 147'328.- en faveur du même compte bancaire ; ces fonds ont été recrédités sur le compte de la lésée ;

4) le 13 janvier 2017, EUR 127'532.- en faveur du compte 21 au nom de la société 17 auprès de la banque 8 à Sofia (BG) ; ces fonds ont été recrédités sur le compte de la lésée ;

5) le 16 janvier 2017, EUR 274'193.- en faveur du même compte ; ces fonds ont été recrédités sur le compte de la lésée (*recte* : ces fonds n'ont pas pu être récupérés ; MPC 10-05-0079 et MPC 05-05-0023) ;

6) le 17 janvier 2017, EUR 296'702.- en faveur du compte 22 au nom de la société 18 auprès de la banque 9 ; ces fonds n'ont pas pu être récupérés (*recte* : ces fonds ont été bloqués et restitués à la lésée ; MPC 05-05-0023) ;

H.1.4 Le préjudice de la société H. s'élève ainsi à EUR 296'702.- (*recte*: EUR 274'193.-). Les débits recrédités s'élèvent à EUR 1'011'866.- (EUR 297'157.- + EUR 143'147.- + EUR 147'328.- + EUR 127'532.- + EUR 296'702.-).

H.2 Des moyens de preuve

H.2.1 Il ressort des avis de détail produits par H. (MPC 05-05-0025) que, par ordres du 4 janvier 2017 exécutés le lendemain, sa relation bancaire 23 a bien été débitée de EUR 297'157.- en faveur du compte n°19 de la société 16 auprès de la banque 7 et de EUR 143'147.- en faveur de la société 12.a., […] Dortmund (D), sur son compte n° 20 auprès de la banque 5, à Francfort-sur-le-Main (D) (MPC 05-05-0036 s.). Ensuite, par ordre du 9 janvier 2017, exécuté le même jour, la même relation de H. a versé EUR 147'328.- à la société 12.a., […] Dortmund (D), sur son même compte, auprès de la banque 5, Francfort-sur-le-Main (D) (MPC 05-05-0036). Par ordres du 13 janvier 2017, la relation de H. a été débitée de EUR 296'702.- en faveur du compte n° 22 au nom de la société 18 auprès de la banque 9 et de EUR 127'532.- en faveur du compte de la société 17, Sofia BG auprès de la banque 8 à Sofia (BG) (MPC 05-05-0038). Le 16 janvier 2017, toujours le même compte de H. a versé un deuxième montant, de EUR 274'193.- sur ce compte de la société 17 (MPC 05-05-0037).

H.2.2 A teneur du journal des appels de H., son raccordement 24 a contacté à 11 reprises le numéro 16 entre le 5 et 16 janvier 2017 (MPC 05-05-0050). La première prise de contact de « M. BB. », le 4 janvier 2017, a été effectuée avec le numéro 17 (MPC 05-05-0029).

H.2.3 Entendue le 20 janvier 2017, SS. a expliqué le déroulement des faits tels que reprochés au prévenu (MPC 05-05-0029 ss). En substance, elle a déclaré avoir été contactée le 4 janvier 2017, entre 15h et 16h, par un certain « M. BB. » de la banque, depuis le raccordement 17. « M. BB. » lui avait alors annoncé qu'il allait faire une mise à jour du logiciel *e-banking*, qui prendrait entre 48h et 72h (MPC 05-05-0029). Elle lui avait encore demandé de lui prouver qu'il appelait de la banque 4, ce sur quoi « M. BB. » avait réagi en lui proposant de la connecter avec la bande-annonce téléphonique de la banque. « M. BB. » lui avait ensuite fait ouvrir une application du type TeamViewer et SS. avait exécuté le programme. Toujours à la demande de « M. BB. », SS. s'était ensuite connectée au portail *e-banking* et avait suivi les instructions de « M. BB. », ensuite de quoi « M. BB. » lui avait indiqué que la mise à jour allait commencer. A sa demande, il l'avait encore accompagnée à travers un processus de paiement et avait remis à SS. un pdf de confirmation des versements effectués. Il lui avait encore indiqué être joignable au numéro 16 si elle devait effectuer d'autres versements pendant la (prétendue) migration et l'avait instruite à ne pas se connecter par elle-même à l'*e-banking*, dans quel cas la mise à jour devrait être recommencée (MPC 05-05-0030 s.). Interpellée par la durée du processus, SS. a recontacté « M. BB. » pour qu'il lui en donne les raisons, sur quoi ce dernier avait fourni plusieurs excuses (MPC 05-05-0032).

H.2.4 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier le détournement de fonds au préjudice de H. (MPC 13-01-0092 et 13-01-0199). Lors de son audition du 28 octobre 2022, le prévenu a finalement admis être « M. BB. » qui avait contacté H. (MPC 13-01-0248).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

I. K. (chiffre 1.3.5 de l'acte d'accusation)

I.1 Des faits reprochés au prévenu

I.1.1 A teneur de l'acte d'accusation, le 9 janvier 2017, à 11h45, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté téléphoniquement la société K. à X. Il s'est présenté sous la fausse identité de « BB.a. », prétendant travailler pour la banque 4, puis a expliqué à TT., responsable comptabilité et finance, qu'il lui était nécessaire de se connecter à l'*e-banking* pour vérifier la version dont disposait la société. Le prévenu a alors demandé à son interlocutrice d'ouvrir son navigateur internet et lui a dicté l'adresse « www.5 » en la priant de cliquer sur l'option « exécuter ». Il lui a ensuite demandé de se connecter au système *e-banking* donnant accès aux comptes de la société auprès de la banque 4. TT. a alors ouvert une session *e-banking* au moyen de ses accès et le prévenu a été en mesure de lui communiquer le solde d'un compte bancaire qui apparaissait sur l'écran. Après cette conversation téléphonique, TT. a appelé la banque 4 qui lui a indiqué que son précédent interlocuteur ne travaillait pas pour elle.

I.1.2 Au moyen de l'adresse URL susmentionnée, le prévenu a ainsi amené TT. à télécharger à son insu un logiciel d'accès à distance sur son ordinateur, grâce auquel il a pu accéder indument au système informatique de la société K. et prendre connaissance de manière illicite de données de la société, en particulier des données bancaires.

I.1.3 Aucun transfert de fonds n'a toutefois pu être ordonné à cette occasion par les autres auteurs.

I.2 Des moyens de preuve

I.2.1 TT. a été entendue le 11 janvier 2017 et ses déclarations quant au déroulement des faits correspondent au comportement reproché au prévenu (MPC 05-02-0049 ss). TT. a ainsi indiqué, en substance, que « BB.a. », de la banque 4, avait contacté la société le 9 janvier à 11h45. Il avait d'abord, de manière détournée, demandé au standard des informations sur l'entreprise et TT., avant d'être mis en relation avec cette dernière. Après l'avoir mise en confiance, « BB.a. » lui avait

alors expliqué que la banque devait effectuer une migration. Il lui avait donné instruction de se rendre sur la page « 5 », soi-disant pour vérifier sa version du logiciel (MPC 05-02-0050). Toujours à la demande de « BB.a. », elle avait alors cliqué sur le bouton « exécuter » apparaissant à l'écran, puis s'était connectée au portail *e-banking*. « BB.a. » l'avait alors accompagnée dans sa navigation sur le portail. Il avait été en mesure de lui donner le solde du compte bancaire s'affichant à l'écran de TT. « BB.a. » lui avait ensuite posé des questions quant aux titulaires des droits de signature sur les comptes de la société. TT. ayant alors eu un mauvais pressentiment et lui ayant demandé une preuve qu'il travaillait bien pour la banque, « BB.a. » lui avait alors proposé de lui envoyer un courriel (MPC 05-02-0051). Ensuite, « BB.a. » avait demandé à TT. de se connecter aux postes de ses collègues pour procéder aux mêmes soi-disant vérifications de la version *e-banking*. TT. ayant prétendu que ses collègues étaient en pause, « BB.a. » l'avait recontactée à 13h30. Dans l'intervalle, TT. avait obtenu la confirmation de la banque 4 que « BB.a. » n'appelait pas pour la banque. Confronté à ce fait, « BB.a. » avait encore prétendu que c'était faux et que, si elle lui donnait le nom de la personne à qui elle avait parlé, il ferait en sorte que la même personne la recontacte pour lui confirmer qu'il travaillait bien pour la banque (MPC 05-02-0051).

I.2.2 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier la prise de contact avec la société K. (MPC 13-01-0092, 13-01-0198). Lors de son audition du 28 octobre 2022, le prévenu a finalement admis être « M. BB. » qui avait contacté K. (MPC 13-01-0248).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

J. B. (chiffre 1.3.6 de l'acte d'accusation)

J.1 Des faits reprochés au prévenu

J.1.1 Selon l'acte d'accusation, à une date indéterminée dans le courant du mois de janvier 2017, depuis un lieu en Israël qui n'a pu être déterminé précisément, l'un des auteurs non identifiés a appelé téléphoniquement la société B. à La Chaux-de-Fonds. Il s'est présenté auprès de la responsable de la comptabilité, AAA., sous l'identité fictive de « M. GG. », employé de la banque 4, annonçant qu'un de ses collègues nommé « BB. », reprendrait contact avec elle pour mettre à jour des clés *e-banking*.

J.1.2 Le 16 janvier 2017, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté téléphoniquement AAA. en se présentant sous l'identité de « M. BB. », prétendument employé par la banque 4. Le prévenu a alors expliqué à la précitée qu'il allait « mettre le système en route », ce qui

provoquerait une interruption de service de 48 à 72 heures. La responsable de la comptabilité devant encore effectuer des paiements pour le compte de B., le prévenu a dû patienter jusqu'au 23 janvier 2017 avant de la rappeler, annonçant qu'il voulait lancer la mise à jour des clés. AAA. a alors collecté 5 des 6 clés permettant d'accéder aux comptes bancaires de l'entreprise par le système *e-banking*. Dans ce contexte, entre le 23 et le 24 janvier 2017, depuis un endroit qui n'a pu être localisé en Israël, le prévenu s'est entretenu par téléphone avec AAA. et l'a convaincue de se connecter elle-même au système *e-banking* de la banque 4 sur les comptes de B. au moyen de sa propre clé ainsi que de celles qu'elle avait collectées. Il l'a ensuite priée d'introduire une adresse URL dans la barre adresse de son navigateur, commençant par « www.6 » et suivie par des chiffres, puis de lui donner accès à distance à son ordinateur au moyen du logiciel TeamViewer, en lui demandant de lui communiquer le numéro d'identification qui s'affichait et le mot de passe qui y figurait, ainsi que d'afficher le clavier numérique sur l'écran avant d'entrer son NIP. Le prévenu a ensuite demandé à son interlocutrice de presser sur la touche F5, ce qui a eu pour effet de rendre noir l'écran de celle-ci. Les 25, 26 et 31 janvier 2017, le prévenu a rappelé téléphoniquement AAA., en la priant de répéter les mêmes opérations, mais uniquement avec sa clé et celle du directeur financier BBB.

J.1.3 Grâce au logiciel de contrôle susmentionné, le prévenu a ainsi indument accédé à l'ordinateur d'AAA. et, partant, au système informatique de B. ; il a par la même occasion pris connaissance sans droit des données bancaires de la société précitée, en particulier des données d'accès au système *e-banking* utilisé par ladite société. Il a également communiqué les données d'accès à l'*e-banking* et l'accès à l'ordinateur d'AAA. aux autres auteurs. Ceux-ci ont alors pu, depuis un endroit en Israël qui n'a pu être déterminé précisément, se connecter à treize reprises directement aux ordinateurs de B. entre le 23 et le 30 janvier 2017. Ils ont de la sorte pu prendre connaissance illégalement des données bancaires de B. et ordonner sans droit 7 transferts de fonds par le débit du compte 25 au nom de la société précitée auprès de la banque 4, pour des montants totaux de EUR 1'124'823.- et CHF 722'151.- selon le détail suivant :

1) le 24 janvier 2017, EUR 192'726.- en faveur du compte 26 au nom de la société 19 à Budapest (HUN) auprès de la banque 10, également à Budapest (HUN) ;

2) le 24 janvier 2017, CHF 328'425.- en faveur du compte 27 au nom de la société 2 auprès de la banque 1 à Genève ;

3) le 25 janvier 2017, EUR 199'726.- en faveur du compte 28 au nom de la société 20 à Düsseldorf (D) auprès de la banque 11 ;

4) le 26 janvier 2017, EUR 182'026.- en faveur du compte 29 au nom de la société 21 à Dahme auprès de la banque 12 à Francfort-sur-le-Main (D) ;

5) le 26 janvier 2017, EUR 197'620.- en faveur du compte 30 au nom de la société 22 à Francfort-sur-le-Main (D) auprès de la banque 5 également à Francfort-sur-le-Main (D) ;

6) le 27 janvier 2017, CHF 393'726.- en faveur du compte 27 au nom de la société 2 auprès de la banque 1 à Genève ;

7) le 31.01.2017, EUR 352'725.- en faveur du même compte au nom de la société 2, bloqué par la banque 4.

J.1.4 Le montant total du préjudice subi par B. s'élève à EUR 925'097.- (*recte* : EUR 772'098.-) et CHF 722'151.-.

J.2 Des moyens de preuve

J.2.1 A l'appui de sa plainte, B. a produit les avis de détails pour les transactions frauduleuses exécutées (MPC 05-00-0020 ss). Il en ressort que son compte lié à l'IBAN 31 a été débité, le 24 janvier 2017, de EUR 192'726.- (montant comptable : CHF 208'716.86) en faveur de la société 19 à Budapest (HUN) sur son compte 26 et de CHF 328'425.- en faveur de la société 2 sur son compte 27, le 25 janvier 2017 de EUR 199'726.- (montant comptable : CHF 216'237.55) en faveur de la société 20 à Düsseldorf (D) sur son compte 28. Le 26 janvier 2017, il a été débité de EUR 182'026.- (montant comptable : CHF 196'595.36) en faveur de la société 21 à Dahme (D) sur son compte 29 et de celui de EUR 197'620.- (montant comptable : CHF 213'694.21) en faveur de la société 22 à Francfort-sur-le-Main (D) sur son compte 30. Finalement, le 27 janvier 2017, la même relation de B. a été débitée de CHF 393'726.- en faveur de la société 2 sur son compte 27. La somme des débits opérés s'élève ainsi à CHF 1'557'394.98.

J.2.2 B. a en outre versé au dossier le journal *e-banking* de la banque 4 relatif au détournement de fonds, qui corrobore les informations ressortant des avis de détail (MPC 05-00-0036 ss).

J.2.3 Il ressort en outre de la documentation produite par la banque 4 que les auteurs se sont bien connectés par 13 fois à l'ordinateur de B. via le logiciel TeamViewer (MPC 10-01-0006).

J.2.4 Entendue le 1er février 2017, AAA. a décrit le déroulement des événements tel qu'il est reproché au prévenu (MPC 05-00-0030 ss). Elle a notamment précisé que la première prise de contact était intervenue par un prétendu « M. GG. » (MPC 05-00-0031). Elle a expliqué avoir eu un dernier contact avec « M. BB. » le 31 janvier 2024, après que la banque avait informé la société B. que ses démarches relevaient d'une fraude. « M. BB. » lui avait alors expliqué que les prélèvements en cause étaient tout à fait normaux, qu'il s'agissait de paiements tests qui n'apparaissaient dès lors pas sur les relevés déposés sur le bureau de son ordinateur. Il lui a encore indiqué que la conseillère clientèle allait lui envoyer

un courriel pour confirmer le bien-fondé et la réalité de ces démarches de mises à jour (MPC 05-00-0032).

J.2.5 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier le détournement de fonds au préjudice de B. (MPC 13-01-0093). Lors de son audition du 28 octobre 2022, le prévenu a finalement admis être « M. BB. » qui avait contacté B. (MPC 13-01-0248, 13-01-0273).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

K. R. (chiffre 1.3.7 de l'acte d'accusation)

K.1 Des faits reprochés au prévenu

K.1.1 A teneur de l'acte d'accusation, le 7 décembre 2017, vers 10h, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté téléphoniquement la société R. à Y. Se présentant sous le pseudonyme de « CC. », prétendument employé à la maintenance technique de la banque 4, il a amené la comptable CCC. à télécharger à son insu le logiciel NTRCloud à 10h08 à l'adresse « 7 », en prétextant la mise en œuvre d'une migration du système *e-banking*. Le prévenu a également prié la comptable de se connecter au système *e-banking* de la banque 4 sur son propre compte et sur celui de sa collègue Mme DDD.

K.1.2 Au moyen du logiciel de contrôle à distance susmentionné, le prévenu a pu accéder indument à l'ordinateur de CCC. et au système informatique de la société susmentionnée, ainsi qu'aux sessions *e-banking* ouvertes par la comptable. Il a ainsi pu prendre connaissance de manière illicite des données de la société R., en particulier des données bancaires de celle-ci. Il a également communiqué les données d'accès à l'*e-banking* et l'accès à l'ordinateur de CCC. aux autres auteurs. Ceux-ci ont alors pu, depuis un endroit en Israël qui n'a pu être déterminé précisément, ordonner de manière illicite le transfert de la somme de EUR 173'428.- par le débit du compte de la banque 4 de la société précitée en faveur du compte 32 au nom de la société 23 à Klettgau (D) auprès de la banque 13 à Constance (D).

K.2 Des moyens de preuve

K.2.1 A l'appui de sa plainte, R. a produit le journal *e-banking* de sa banque pour les transactions frauduleuses (MPC 05-04-0006 ss) ainsi que les détails de la transaction en cause (avis et swift). Il en ressort que, par ordre du 7 décembre 2017, les auteurs ont donné instruction à la banque de verser EUR 173'428.- du compte de R. 33 sur le compte 32 de la société 23 (D) logé

auprès de la banque 13 à Constance (D), mais que le paiement n'a pas été exécuté (MPC 05-04-0008 s. et 10-08-0019).

K.2.2 Il ressort de l'analyse technique effectuée par la PJF sur l'ordinateur de CCC. qu'en date du 7 décembre 2017, entre 10h08 et 10h38, l'appareil s'est connecté à la page « 7 » et a téléchargé le logiciel NTRCloud, grâce auquel les auteurs se sont simultanément connectés à l'ordinateur de CCC. par l'adresse IP 34 appartenant au provider israélien société 24 (MPC 10-02-0307 s.).

K.2.3 Entendue le 16 février 2018, CCC. a décrit les événements correspondant aux agissements reprochés au prévenu (MPC 05-04-0001 ss). Elle a ainsi expliqué, en substance, que « CC. », appelant prétendument de la maintenance technique de la banque 4, l'avait contactée le 7 décembre 2017 et lui avait demandé de se connecter au site « 7 » depuis son poste de travail, puis de faire de même depuis le poste de sa collègue. Il lui avait ensuite indiqué qu'il rappellerait en début d'après-midi. Ensuite de cet appel, elle avait été contactée par la banque au sujet de l'ordre de transaction en faveur de la société 23 (D), qu'elle avait alors refusé (MPC 05-04-0001 s.).

K.2.4 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier la prise de contact avec R. (MPC 13-01-0095). Lors de son audition du 28 octobre 2022, le prévenu a finalement admis être « M. CC. » qui avait contacté R. (MPC 13-01-0249, 13-01-0274).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

L. N. (anc. N.a.) (chiffre 1.3.8 de l'acte d'accusation)

L.1 <u>Des faits reprochés au prévenu</u>

L.1.1 A teneur de l'acte d'accusation, le 20 décembre 2017, vers 11h, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté téléphoniquement la société N.a., devenue par la suite N., à Z., sous le pseudonyme de « CC. », en prétendant travailler au service informatique de la banque 14. Il a ainsi indiqué à EEE., employée de la société, que le logiciel de comptabilité de cette dernière devait être mis à jour, puis lui a demandé de se connecter à l'adresse URL « www.8 ». Il lui a encore fait effectuer plusieurs manipulations sur son ordinateur, la priant notamment de scanner un document mentionnant ses données d'utilisation du logiciel avant de terminer la prétendue mise à jour. Au moyen de l'adresse URL précitée, le prévenu a ainsi amené EEE. à télécharger à son insu le logiciel de contrôle à distance NTRCloud, lequel lui a permis de pénétrer sans droit dans le système informatique de la société et de

prendre connaissance de données spécialement protégées, en particulier les données bancaires et les données d'accès à l'*e-banking*.

L.1.2 EEE. a toutefois pris contact avec la banque 14 pour vérifier les dires du nommé « CC. » et l'accès aux comptes a été bloqué par la banque, empêchant ainsi tout transfert de la part des auteurs.

L.2 Des moyens de preuve

L.2.1 Entendue le 27 décembre 2017, EEE. a décrit les événements tels que reprochés au prévenu (MPC 05-03-0011 s.). En substance, elle a expliqué que « CC. » du service informatique de la banque 14 l'avait contactée le 20 décembre 2017 en lui expliquant qu'il fallait faire une mise à jour du logiciel. Il lui avait alors fait faire plusieurs manipulations et lui a fait scanner le document comprenant ses données d'utilisatrice. Elle a alors convenu avec « CC. » qu'il la rappellerait après la pause de midi pour procéder à la mise à jour sur le poste d'une collègue (MPC 05-03-0011). Après avoir été mise en garde par un collègue, EEE. avait contacté la banque puis découvert une fenêtre sur son bureau, nommée « NTR Global ». Ensuite, la société avait procédé au contrôle de tous les paiements en attente et des montants des différents comptes, ceci sans découvrir de transaction douteuse (MPC 05-03-0012).

L.2.2 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier la prise de contact avec la société N.a., devenue N. (MPC 13-01-0095). Lors de son audition du 28 octobre 2022, le prévenu a finalement admis être « CC. » qui avait contacté N.a. (MPC 13-01-0249).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

M. C. (chiffre 1.3.9 de l'acte d'accusation)

M.1 Des faits reprochés au prévenu

M.1.1 A teneur de l'acte d'accusation, le 16 mai 2018, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté téléphoniquement la société C. à Genève. Il s'est alors présenté au responsable de la comptabilité de la société précitée, FFF., sous le pseudonyme de « BB. », prétendument responsable du service *e-banking* de la banque 4, lui annonçant qu'une migration du système *e-banking* devait avoir lieu à la banque 4 dès le 22 mai 2018. Le lendemain 17 mai, le prévenu a rappelé FFF. et lui a demandé de se connecter à l'adresse « www.9 », au moyen de laquelle il a amené son interlocuteur à télécharger à son insu le logiciel de contrôle à distance NTRCloud sur son ordinateur. Le 22 mai 2018, le prévenu a à nouveau contacté FFF.

téléphoniquement en lui demandant de se connecter au portail *e-banking* de la banque 4 au moyen des accès de GGG., administrateur de C. seul habilité à valider les paiements. Après diverses vérifications demandées à FFF., le prévenu l'a prié de récupérer les cartes *e-banking* auprès de ses collègues afin d'empêcher tout accès électronique aux comptes durant 72 heures, condition du succès de la migration selon lui. Lors de cette conversation et au moyen du logiciel NTRCloud, le prévenu a accédé indument à l'ordinateur de FFF. et, partant, au système informatique de la société susmentionnée ; il a ainsi pris connaissance des données d'accès *e-banking* de FFF. et de GGG. aux comptes de la société auprès de la banque 4, à l'insu de ces derniers.

M.1.2 Le 23 mai 2018, le prévenu a appelé FFF. à plusieurs reprises. Dans l'après-midi, après avoir ouvert deux sessions *e-banking* au moyen des accès de FFF. et de GGG., illicitement obtenus comme indiqué plus haut, il a prié son interlocuteur de lui communiquer les « codes challenge », soit les codes de double authentification permettant l'accès *e-banking*, qui s'affichaient sur sa calculette de la banque 4, puis sur celle de GGG. Le prévenu a ensuite remis ces données aux autres auteurs afin de leur permettre de transférer des fonds sans droit depuis les comptes de C. à leur profit, comme décrit ci-après. Le prévenu a encore appelé quotidiennement FFF. jusqu'au 31 mai 2018, afin notamment d'effectuer des paiements urgents par les comptes de la société, à la demande de FFF.

M.1.3 Entre le 22 et le 31 mai 2018, depuis un lieu indéterminé en Israël, au moyen des accès *e-banking* obtenus sans droit par le prévenu, les autres auteurs ont pu ordonner, indument et à l'insu des responsables et employés de C., les transferts suivants par le débit des comptes de la société :

1) le 22 mai 2018 : EUR 318'209.- en faveur du compte no 35 auprès de la banque 15 à Prague (CZ) au nom de la société 25 dans la même ville ;

2) le 24 mai 2018 : EUR 389'147.- en faveur du compte du même compte au nom de la société 25 à Prague (CZ) ;

3) le 28 mai 2018 : EUR 287'452.- en faveur du compte n° 36 auprès de la banque 16 à (HK) au nom de la société 26 ;

M.1.4 Le montant total du préjudice s'élève ainsi à EUR 994'808.- (EUR 318'209.- + EUR 389'147.- + EUR 287'452.-) [dont EUR 920'808.-, soit EUR 994'808.- - EUR 74'000.-, n'ont pu être bloqués ; cf. ch. M.2.2 *infra*].

M.2 Des moyens de preuve

M.2.1 A l'appui de sa plainte, C. a produit les swifts pour les transactions frauduleuses en cause (MPC 10-02-0137 ss). Il en ressort que la relation de C. a bien été débitée, par ordre du 22 mai 2018 exécuté le même jour, d'un montant de

EUR 318'209.- en faveur de la société 25, IBAN n° 35 auprès de la banque 15 à Prague (CZ) (MPC 10-02-0137), puis d'un montant de EUR 389'147.-, par ordre du 24 mai 2018 exécuté le même jour, en faveur de la même relation bancaire de la société 25 (MPC 10-02-0138). Finalement, le compte de C. a été débité de EUR 287'452.- par ordre du 28 mai 2018 exécuté le 30 mai 2018, ledit montant ayant bien été versé à la société 26 (MPC 10-02-0139).

M.2.2 Il ressort des actes d'entraide effectués par les autorités tchèques que le compte n° 35.a. de la société 25 dans les livres de la banque 15 à Prague (CZ) a été crédité de deux virements du compte C., soit un versement d'EUR 318'199.- le 22 mai 2018 et un versement de EUR 389'137.- le 25 mai 2018 (MPC 18-07-0094 s. et 18-07-0074). Ces fonds ont ensuite pour partie été transférés sur les comptes n° 37 au nom de la société 27 par EUR 64'941.10, n° 38 au nom de la société 28, par EUR 319'000.-, n° 39 au nom de HHH. par EUR 236'500.- et n° 40 au nom de la société 29, par EUR 74'000.- (MPC 18-07-0095 s.). Les fonds provenant de cette dernière transaction ont été retournés à la banque 15 (CZ) à raison d'EUR 73'860.-, puis bloqués par les autorités tchèques (MPC 18-07-0096 s.). Ils ont d'ores et déjà été restitués à la lésée (MPC 18-07-0141 ss et 15-04-0231).

M.2.3 Il ressort ensuite de la documentation bancaire remise par les autorités chinoises, que la relation de la société 26 auprès de la banque 16 (HK) a bien reçu un versement de EUR 287'342.- le 31 mai 2018 en provenance du compte de C., n° 41 (MPC 18-10-0105 s.).

M.2.4 La PJF a procédé à une analyse forensique de l'ordinateur de FFF. (MPC 10-02-127 et 10-02-308 ss). Il en ressort plusieurs visites du site tinyurl.com et le téléchargement coïncident du logiciel NTRCoud, précédé ou suivi de l'ouverture d'une session *e-banking* de la banque 4, puis d'une activité *e-banking*, le 17 mai 2018, de 9h59 à 10h02 et le 22 mai 2018, de 09h18 à 10h15 (MPC 10-02-0309 s.). Par quatre fois ultérieurement, soit les 23, 24, 28 et 31 mai 2018, l'ordinateur de FFF. se connecte tinyurl.com, ensuite de quoi il est redirigé vers le site partage-fichiers.com. A tout le moins le quatrième fichier, nommé « Paiementnational_20180529_1558.pdf » correspond à une preuve d'ordre de virement pour une société située en Suisse (MPC 10-02-0310).

M.2.5 Entendus le 6 juin 2018, GGG. (MPC 05-06-0001 ss et 12-10-0001 ss) et FFF. (MPC 12-09-0001 ss) ont expliqué le déroulement des événements de manière concordante avec les faits reprochés au prévenu. Ainsi, FFF. a expliqué avoir été contacté le 16 mai 2018, à 11h22 par un certain « M. BB. » de la banque 4, en vue d'effectuer une migration *e-banking*. « M. BB. » avait d'emblée précisé qu'aucun collaborateur ne devait se connecter au portail *e-banking* au cours de la migration (MPC 12-09-0003). Le lendemain, « M. BB. » avait recontacté FFF., lui avait dicté une URL, « 35 », à laquelle FFF. s'était alors connecté, sur instruction de « M. BB. ». Le 22 mai 2018, « M. BB. » l'avait à nouveau appelé et

lui avait demandé de se connecter au portail *e-banking* de la société, à l'aide de ses codes d'accès, ensuite de quoi, « M. BB. » l'avait guidé sur l'interface *e-banking*. A l'issue de ces démarches, « M. BB. » avait encore précisé à FFF. que la migration durerait 72 heures (MPC 12-09-0004). Le lendemain 23 mai 2023, « M. BB. » avait à nouveau contacté FFF. et lui avait demandé son code d'accès à la session *e-banking*, tel que fourni par la calculette, ainsi que celui de GGG. (MPC 12-09-0005). Au cours de la soi-disant migration, FFF. et « M. BB. » ont été en contact afin que ce dernier puisse procéder à des versements urgents, tels que demandés par FFF. (MPC 12-09-0006). GGG. a, pour sa part, confirmé s'être connecté à sa session *e-banking* le 22 mai 2018, à la demande de « M. BB. ». Ce dernier lui avait alors demandé de confirmer certains éléments visibles sur la page. Au cours de cet échange, « M. BB. » lui avait demandé, à une ou deux reprises, d'appuyer sur l'une des touches F situées en haut du clavier (MPC 12-10-0003).

M.2.6 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier le détournement de fonds au préjudice de C. (MPC 13-01-0095 s. et 13-01-0203 s.). Lors de son audition du 28 octobre 2022, le prévenu a décidé de s'expliquer et a admis certains cas (MPC 13-01-0236). Toutefois, il a alors persisté à nier toute implication dans le détournement des fonds de C., faute d'avoir – selon ses dires – reçu de « commission » – c'est-à-dire une part du butin – correspondant au détournement de fonds au préjudice de C. (MPC 13-05-0078 et 13-01-0274 s.). Le 10 novembre 2022, le prévenu a enfin admis être la personne qui avait appelé la société C. et avoir participé à la réalisation de ce cas (MPC 13-01-0279). Il a spontanément expliqué avoir nié toute implication dans ce volet – y compris après avoir annoncé au MPC qu'il entendait s'expliquer, le 28 octobre 2022 – parce qu'il n'avait « pas touché un euro », s'étant « embrouillé avec EE. » et que ce dernier ne lui avait rien donné comme « commission » sur ce cas-là (MPC 13-01-0279 et 13-01-0299).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

N. L. (chiffre 1.3.10 de l'acte d'accusation)

N.1 <u>Des faits reprochés au prévenu</u>

N.1.1 A teneur de l'acte d'accusation, le mardi 29 mai 2018, depuis un lieu en Israël qui n'a pu être déterminé précisément, l'un des auteurs non identifiés a appelé téléphoniquement la société L. à Genève. Il s'est présenté auprès du directeur financier III. en affirmant faussement se nommer « GG. » et représenter la banque 4, annonçant qu'un de ses collègues du service technique nommé « BB. » reprendrait contact avec lui. Quelques minutes plus tard, à Netanya (IL),

le prévenu a contacté téléphoniquement III. sous la fausse identité de « BB. » en affirmant qu'une migration du système *e-banking* allait avoir lieu, puis l'a prié de se rendre sur un site dont il lui a dicté l'adresse – laquelle n'a pas pu être identifiée – en lui indiquant qu'il s'agissait d'un site permettant d'obtenir les « clés de migration ». Le prévenu a ainsi amené III. à télécharger à son insu le logiciel de contrôle à distance NTRCloud. Il lui a ensuite demandé de se connecter au compte *e-banking* de la société précitée au moyen de sa calculette, puis d'ouvrir une session *e-banking* avec les accès de JJJ., directeur général ; ce dernier a remis ces informations et sa calculette à III. qui a ouvert une nouvelle session sur son ordinateur également. Le prévenu a de la sorte pu accéder indument à l'ordinateur d'III. et, partant, au système informatique de la société susmentionnée ; il a ainsi pu prendre connaissance de données de la société, en particulier les données bancaires. Il a encore indiqué à son interlocuteur que la migration allait durer entre 48 et 72 heures et qu'il ne devait pas se connecter durant cette période.

N.1.2 Le même jour, depuis un lieu indéterminé en Israël, le prévenu a remis les données d'accès susmentionnées aux autres auteurs qui ont ainsi pu se connecter à l'ordinateur d'III., le même jour entre 9h58 et 10h12, puis à la session *e-banking* ouverte par ce dernier, entre 10h00 et 10h11. Ce faisant, les auteurs ont pris connaissance indument des données bancaires de la société L. et ont procédé sans droit à un transfert de EUR 97'254.- en faveur du compte n° 42 au nom de la société 30 auprès de la banque 17 à Londres (UK).

N.2 Des moyens de preuve

N.2.1 La lésée a produit l'avis de détail pour la transaction frauduleuse en cause, ainsi que le log *e-banking* correspondant. Il en découle que le compte n° 43 ouvert dans les livres de la banque 4 au nom de L. a bien été débité de la somme de EUR 97'254.- par ordre du 29 mai 2018 exécuté le même jour, en faveur de la relation de la société 30 (MPC 10-02-0161), sur son compte auprès de la banque 17 (MPC 10-02-0166).

N.2.2 La PJF a effectué une analyse forensique de l'ordinateur d'III. (MPC 10-02-0160). Il en ressort que, le 29 mai 2018, il y a eu connexion à distance NTRCloud sur l'appareil, entre 9h58 et 10h12. Dans cet intervalle, une activité *e-banking* de la banque 4 a également été enregistrée, entre 10h00 et 10h11 (MPC 10-2-0313 s.).

N.2.3 Lors de son audition du 7 juin 2018, III. a, en substance, décrit la prise de contact telle que reprochée au prévenu (MPC 12-11-0003 ss). Il a ainsi expliqué que, le 29 mai 2018, vers 11h35, un certain « GG. » de la banque 4 l'avait appelé pour lui annoncer que « BB. » le contacterait. Quelques minutes plus tard, « BB. » l'avait appelé et lui avait parlé d'une migration *e-banking*, avant de lui dicter un site internet, (prétendument) pour obtenir des clés de migration. Après avoir tapé

l'URL dictée par « BB. » dans la barre d'adresse, III. s'était alors connecté au portail *e-banking*, toujours sous instructions de « BB. ». « BB. » l'avait alors accompagné dans sa navigation sur le portail, avant de lui indiquer que la migration allait durer entre 48h et 72h, au cours desquelles personne ne devait se connecter au portail (MPC 12-11-0003). Toujours à la demande de « BB. », III. a procédé aux mêmes manipulations, sur son poste, avec les identifiants *e-banking* de son collègue JJJ. (MPC 12-11-0004).

N.2.4 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier le détournement de fonds au préjudice de L. (MPC 13-01-0096). Lors de son audition du 28 octobre 2022, le prévenu a finalement admis être « BB. » qui avait contacté L. (MPC 13-01-0247).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

O. D. (chiffre 1.3.11 de l'acte d'accusation)

O.1 Des faits reprochés au prévenu

O.1.1 A teneur de l'acte d'accusation, le 7 juin 2018, depuis un lieu en Israël qui n'a pu être déterminé précisément, l'un des auteurs non identifiés a appelé téléphoniquement la société D. à Genève. Il s'est présenté auprès de la réception, puis de la comptable KKK. en affirmant faussement se nommer « GG. » et travailler pour une société de services informatiques mandatée par la banque 4 afin d'effectuer une migration informatique en lien avec les services d'*e-banking*. L'individu l'informant que la migration entraînerait un blocage de l'utilisation de l'*e-banking* durant 48 heures, la comptable lui a indiqué qu'elle n'était pas habilitée à l'autoriser et l'a prié d'envoyer un courriel à l'office manager de la société.

O.1.2 L'après-midi du même jour, l'individu a rappelé KKK. et lui a passé le prévenu en le présentant sous le faux nom de « BB. », prétendument chargé des aspects techniques de la migration. Celui-ci a alors amené la comptable à télécharger le logiciel NTRCloud à son insu au moyen du lien raccourci « www.10 » sous prétexte de lui communiquer un « numéro de migration » et lui a donné quelques explications sur le déroulement de l'opération. Le prévenu, ainsi que les autres auteurs auxquels il a remis les accès, ont de la sorte pu indument accéder une première fois à l'ordinateur de KKK. et, partant, au système informatique de la société susmentionnée, au moyen du logiciel NTRCloud, le même jour, entre 14h01 et 14h09, et prendre ainsi illicitement connaissance des données qu'il contenait, en particulier les données d'accès à l'*e-banking*, lors de la session ouverte de 14h02 à 14h08 sur l'ordinateur de la comptable.

O.1.3 Le prévenu a derechef contacté téléphoniquement KKK. le 11 juin 2018 en lui indiquant que la migration allait commencer. Le même jour, les autres auteurs ont ouvert une session *e-banking* au moyen des accès de la comptable et le prévenu a communiqué à cette dernière le code produit par cette opération. KKK. a entré ce code sur la calculette de la banque 4 et communiqué au prévenu le « code challenge » généré par cette dernière. Le prévenu a alors remis l'accès ainsi obtenu à l'ordinateur de KKK. et à la session *e-banking* ouverte par celle-ci aux autres auteurs, qui ont pu accéder aux comptes de D. auprès de la banque 4 via le système *e-banking* et ont ordonné illicitement les transferts suivants :

1) le 11 juin 2018 : EUR 98'209.- en faveur du compte n° 44 au nom de la société 31 auprès de la banque 18 à Varsovie (PL) ;

2) le 12 juin 2018 : EUR 96'194.- en faveur du compte n° 45 au nom de la société 32 auprès de la banque 19 à Wroclaw (PL) – versement bloqué par la banque 4 avant son envoi ;

3) le 12 juin 2018 : EUR 99'307.- en faveur de la société 31 sur le compte mentionné ci-dessus – montant bloqué en Pologne et retourné à la banque 4.

O.1.4 Les versements des 12 juin 2018, soit EUR 195'501.- (EUR 96'194.- + EUR 99'307.-) ont pu être bloqués (MPC 10-02-0116). Le préjudice subi par la société D. s'élève ainsi à EUR 98'209.-.

O.2 Des moyens de preuve

O.2.1 Il ressort des logs *e-banking* et des extraits de swifts produits par D. (MPC 10-02-0171 ss), que la relation de D. a été débitée le 11 juin 2018 de EUR 98'209.- en faveur du compte de la société 31 auprès de banque 18, n° IBAN 44 (MPC 10-02-0173 et 10-02-0181). Le 12 juin 2018, il a été donné ordre à la banque d'effectuer, depuis la relation de D., un deuxième versement sur le même compte de la société 31, d'un montant de EUR 99'307.-, ainsi que de verser EUR 96'194.- en faveur de la société 32 auprès de la banque 19 (MPC 10-02-0174 s. et 10-02-0179 s.).

O.2.2 La PJF a procédé à une analyse forensique de l'ordinateur de KKK. (MPC 10-02-0170, 10-02-0055 et 10-02-0316 ss). Il en est ressorti que, le 7 juin 2018, à 14h01, l'appareil s'est connecté au site tinyurl.com, puis a téléchargé le logiciel NTRCloud. Quelques secondes plus tard, ledit logiciel a été exécuté et les auteurs ont ainsi établi une connexion à distance avec l'appareil de KKK. L'adresse IP des auteurs correspond à une adresse IP israélienne provenant de la plage d'adresses IP 46 appartenant au provider israélien société 24 (MPC 10-02-0316 ss).

O.2.3 Entendue le 14 juin 2018, KKK. a, en substance, décrit le comportement reproché au prévenu (MPC 12-13-0001 ss). Elle a ainsi expliqué qu'après une première prise de contact, « GG. » lui avait passé « BB. », qui s'était présenté comme la personne en charge des aspects techniques de la migration à effectuer (MPC 12-13-0004). « BB. » lui avait ensuite communiqué un numéro de migration à noter. Il avait rappelé le lendemain 8 juin 2018, pour commencer la migration (MPC 12-13-0004). « BB. » s'était alors enquis de la nécessité d'effectuer des paiements, ceux-ci n'étant, selon ses dires, pas possible pendant la migration, qui devait durer 48 heures. « BB. » avait alors bien précisé que KKK. ne devait absolument pas se connecter à l'*e-banking* pendant le processus de migration. Agissant toujours sur instruction de « BB. », KKK. avait introduit le code dicté par celui-ci dans sa calculette, puis lui avait transmis le « code challenge » qui s'était affiché. Le lundi suivant, après que KKK. avait pu effectuer un dernier paiement urgent, « BB. » l'avait alors informée que la migration débutait (MPC 12-13-0005). Recontacté dans la semaine par KKK. au sujet de versements à effectuer pendant la migration, « BB. » l'avait assistée et lui avait proposé de lui fournir les preuves de transactions, lui demandant à nouveau de se connecter sur le site tinyurl (MPC 12-13-0006).

O.2.4 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier le détournement de fonds au préjudice de D. (MPC 13-01-0097 et 13-01-0198). Lors de son audition du 28 octobre 2022, le prévenu a finalement admis être le dénommé « BB. », qui avait contacté D. (MPC 13-01-0247).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

P. E. (chiffre 1.3.12 de l'acte d'accusation)

P.1 Des faits reprochés au prévenu

P.1.1 A teneur de l'acte d'accusation, le 7 juin 2018, depuis un lieu en Israël qui n'a pu être déterminé précisément, l'un des auteurs non identifiés a appelé téléphoniquement la société E. à Nyon. Il s'est présenté auprès de LLL., comptable de la société, en affirmant faussement se nommer « GG. » et représenter la banque avec laquelle travaillait la société. Il lui a encore annoncé qu'un nommé « BB. » allait la rappeler en vue de procéder à une mise à jour du système *e-banking*. Quelques instants plus tard, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a appelé LLL. en se présentant sous le pseudonyme de « BB. », prétendument représentant de la banque 4, et en lui posant diverses questions sur le système *e-banking*. Le prévenu a ensuite prié la comptable de se connecter à l'*e-banking*, puis lui a demandé d'ouvrir une nouvelle page sur son navigateur internet. Il l'a également amenée à son insu à

télécharger le logiciel d'accès à distance NTRCloud en l'invitant à se connecter à l'adresse « 11 » qu'il lui a dictée, puis l'a amenée à lui donner le contrôle de son ordinateur, toujours sans qu'elle ne s'en aperçoive.

P.1.2 Il est reproché au prévenu d'avoir ainsi, à la date précitée, entre 10h03 et 10h14, depuis un lieu en Israël qui n'a pu être déterminé précisément, pu accéder indument à l'ordinateur de LLL. et prendre connaissance illicitement de données de E., en particulier des données bancaires auprès de la banque 4.

P.1.3 Toujours selon l'acte d'accusation, Le prévenu a ensuite demandé à LLL. d'ouvrir une session *e-banking* sur la plateforme de la banque 14, au moyen des accès de l'un de ses collègues. Il a alors dicté l'adresse URL « 12 » entraînant le téléchargement de NTRCloud. Le collègue de LLL. a ensuite utilisé ses données d'accès pour ouvrir une session *e-banking* auprès de la banque 14 sur le poste de la comptable. Entre 10h15 et 10h24, le prévenu a ainsi à nouveau pu accéder indument à l'ordinateur de LLL. et, partant, au système informatique de la société susmentionnée ; il a de la sorte pu prendre connaissance illicitement de données de E., en particulier des données bancaires auprès de la banque 14.

P.1.4 Le prévenu a également communiqué ces accès aux autres auteurs qui ont pu se connecter à l'ordinateur de LLL. et aux sessions *e-banking* qu'elle avait ouvertes, avant d'ordonner par ce moyen le transfert du montant de EUR (*recte* : CHF) 720'000.- (MPC 10-08-0019 et 12-17-0004) par le débit du compte de la banque 4 de la société en faveur d'un tiers non identifié. Ce transfert a toutefois été bloqué par la banque, dès lors qu'il manquait une seconde validation par *e-banking*.

P.2 <u>Des moyens de preuve</u>

P.2.1 La PJF a procédé à une analyse forensique de l'ordinateur de LLL. (MPC 10-02-0186 et 10-02-0315 ss). Il en ressort que l'appareil s'est connecté, par deux fois, au site tinyurl.com le 7 juin 2018, une première fois à 10h03, puis à 10h15. Coïncidemment à chacune des deux visites du site tinyurl, l'appareil a téléchargé le logiciel NTRCloud, ensuite de quoi l'appareil a connu une activité *e-banking*, auprès de la banque 4 (après la première connexion à NTRCloud) et auprès de l'*e-banking* de la banque 14 (après la seconde connexion à NTRCloud) (MPC 10-02-0315). La PJF a constaté que les adresses IP utilisées pour se connecter à l''ordinateur de LLL. par l'entremise du logiciel NTRCloud proviennent de la plage d'adresses IP 46 appartenant au provider israélien société 24 (MPC 10-02-0315).

P.2.2 Il est également ressorti des investigations policières que, le 7 juin 2018 également, que l'ordre de transfert de CHF 720'000.-, correspondant environ au solde des avoirs sur le compte, a bien été passé mais n'a pas été exécuté, faute de seconde validation (MPC 10-05-0050 et 10-05-0078).

P.2.3 Entendue le 21 juin 2018, LLL. a, en substance, indiqué avoir reçu un appel d'une personne se présentant comme « GG. » le jeudi 7 juin 2018, entre 11h45 et 12h00. « GG. » s'était annoncé comme appelant de la banque et lui avait indiqué qu'un certain « BB. » allait la rappeler pour procéder à une mise à jour du système *e-banking*. Quelques 10 ou 15 minutes plus tard, un individu se présentant comme « BB. » avait alors appelé LLL., se référant à la conversation qu'elle avait eu avec « GG. ». « BB. » avait alors posé beaucoup de questions à LLL. quant à la convivialité du système, les paiements à effectuer et la version du logiciel *e-banking* de la banque 4. « BB. » s'était renseigné sur la fréquence des versements par la relation bancaire de la banque 4 et les personnes ayant accès à l'ebanking. « BB. » avait ensuite demandé à LLL. de dire à son directeur financier, MMM., de ne pas aller en pause, car – selon « BB. » – il devrait aussi intervenir sur le poste de MMM. « BB. » avait ensuite demandé à LLL. de se connecter à l'ebanking, ce que cette dernière avait fait. Il lui avait alors dicté un lien URL à taper dans la barre de recherche. « BB. » avait ensuite guidé LLL. dans sa navigation sur la page. Soudain, en marge de nouvelles questions quant à la fréquence des opérations sur le compte de la banque 4, « BB. » avait commencé à parler à LLL. de la banque 14. Il avait alors demandé à LLL. qu'elle dise à son collègue ayant accès au compte de la société auprès de la banque 14 de se connecter à l'ebanking de cette banque sur le poste de LLL. Ils effectueraient la même manipulation, ce que LLL. et ledit collègue ont fait. « BB. » a alors annoncé à LLL. qu'elle disposait désormais de la dernière version du logiciel (MPC 12-17-0003 s.). Quelques jours plus tard, le patron de LLL. informait les employés d'une tentative d'escroquerie sur le compte de la banque 4 de la société, pour un montant de CHF 720'000.-. « BB. » l'avait par la suite à nouveau contactée téléphoniquement pour le processus de migration, lui demandant de se reconnecter à l'*e-banking* de la société, ce qu'elle avait refusé, sous prétexte d'un problème technique. En bruit de fond, il lui avait alors passé un film pornographique (MPC 12-17-0004 ; enregistrement audio en annexe au rapport de la PJF du 14 octobre 2021, MPC rubrique 10-02).

P.2.4 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier la prise de contact avec la société E. (MPC 13-01-0096 et 13-01-0197). Lors de son audition du 28 octobre 2022, le prévenu a finalement décidé de s'expliquer (MPC 13-01-0236). Il a alors admis être « BB. » qui avait contacté E. (MPC 13-01-0247).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

Q. O. (chiffre 1.3.13 de l'acte d'accusation)

Q.1 Des faits reprochés au prévenu

Q.1.1 A teneur de l'acte d'accusation, le 13 juin 2018, entre 15h et 16h, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté la société O. à UU. Se présentant sous le pseudonyme de « BB. » et affirmant travailler pour la banque 14, le prévenu s'est entretenu avec NNN., comptable, en lui indiquant que la plateforme *e-banking* de la banque serait bloquée pendant 48 à 72 heures en raison d'une migration. A sa demande, NNN. a tenté d'ouvrir une session *e-banking* à deux reprises, mais sans y parvenir. Le prévenu lui a dès lors dicté l'adresse URL « 13 » au moyen de laquelle le comptable a téléchargé à son insu le logiciel de contrôle à distance NTRCloud. A la demande du prévenu, NNN. a ensuite ouvert une session *e-banking* sur le site de de la banque 14 au moyen de ses données d'accès et a constaté que son interlocuteur voyait ce qui s'affichait sur son écran. Le prévenu lui a alors indiqué diverses manipulations à effectuer dans l'*e-banking*, qui lui ont permis d'accéder directement et indument à l'ordinateur de NNN. et, partant, au système informatique de la société susmentionnée, ainsi qu'à la session *e-banking* qu'il avait ouverte. Le prévenu a encore prié OOO., supérieure de NNN., d'ouvrir également une session *e-banking* sur l'ordinateur de ce dernier, lui permettant ainsi d'obtenir la validation des transferts que les auteurs projetaient d'ordonner au débit des comptes de la société.

Q.1.2 Toujours selon l'acte d'accusation, au moyen de ces accès obtenus illicitement, le prévenu a pu pénétrer sans droit dans le système informatique de O. le 13 juin 2018 et prendre connaissance illicitement de données de la société, en particulier des données bancaires. Il a également communiqué les accès ainsi obtenus aux autres auteurs, leur permettant de la sorte de pénétrer sans droit à plusieurs reprises entre le 13 et le 15 juin 2018 dans le système informatique de la société précitée et d'ouvrir des sessions *e-banking*, d'accéder aux comptes de cette dernière auprès de la banque 14 et d'ordonner les transferts suivants, qui ont toutefois été bloqués *in extremis* par la banque :

1) le 14 juin 2018 : EUR 618'429.- en faveur du compte 47 au nom de la société 33 auprès de la banque 15 à Prague (CZ) ;

2) le même jour : EUR 493'625.73 en faveur du même compte.

Q.2 Des moyens de preuve

Q.2.1 La PJF a procédé à une analyse forensique d'une copie miroir de l'ordinateur de NNN. (MPC 10-02-0077 et 10-02-0318 ss). Il en ressort que l'appareil a visité le site tinyurl.com en date du 13 juin 2018, 14h05. Parallèlement, le logiciel NTRCloud a été téléchargé et exécuté. Il s'ensuit une activité *e-banking* sur le portail de la banque 14, de 14h08 à 15h15. Le 15 juin 2018 également,

l'ordinateur se connecte à 9h17 au site tinyurl.com et, de manière coïncidente, télécharge le logiciel NTRCloud, qui est exécuté (MPC 10-02-0319 s.). Les adresses IP opérateur lors des connexions proviennent de la plage d'adresses IP 46 appartenant au provider israélien société 24 (MPC 10-02-0319 s.).

Q.2.2 A compter du 13 juin 2018, des mesures de surveillance ont été effectuées sur le raccordement 9 (MPC 10-02-0200 ss). Le 14 juin 2018, un individu se présentant comme « M. BB. » contacte NNN. et discute de diverses transactions, s'enquiert de la nécessité pour NNN. de se connecter au compte de la banque 14, indique que la migration est en cours et annonce qu'il rappellera le lendemain (MPC 10-02-0201 ; rubrique 13, ID 1000048631703). Le 18 juin 2018, à 11h08, « M. BB. » rappelle et demande à parler à NNN. et, celui-ci étant absent, à OOO., en se montrant insistant (MPC 10-02-0202 s. et 10-02-0230 ss ; rubrique 13, ID 1000048866970).

Q.2.3 Entendu le 15 juin 2018 (MPC 05-09-0001 ss), PPP., Directeur financier de la lésée, a expliqué qu'une fois avisé de la fraude par la PJF, le 14 juin 2018, il a effectué un contrôle en se connectant à l'interface *e-banking* de la banque 14. Il a alors constaté qu'un virement d'environ CHF 720'000.- était enregistré et apparaissait comme « en suspens » sur ledit interface (MPC 05-09-0002 s.). La banque a ensuite confirmé que le versement avait été bloqué (MPC 05-09-0003, 10-02-0120 et 10-02-0125).

Q.2.4 NNN. a été auditionné le 15 juin 2018 (MPC 12-14-0001 ss). Il a en substance indiqué avoir reçu l'appel d'un individu s'étant annoncé comme étant « M. BB. », le 13 juin 2018. « M. BB. » lui avait demandé s'il y avait des ralentissements ou des problèmes lorsque NNN. effectuait des paiements depuis la plateforme *e-banking* de la banque 14. Il lui avait aussi indiqué que la plateforme *e-banking* allait être bloquée pendant 48 à 72 heures, en raison d'une migration. Ensuite, « M. BB. » avait demandé à NNN. de se connecter à sa session *e-banking*, sans succès, sur quoi « M. BB. » avait rebondi en lui disant que ça irait autrement et en lui dictant une adresse URL tinyurl.com que NNN. avait alors tapée, à la demande de « M. BB. », dans sa barre d'adresse. NNN. avait alors pu se connecter au portail d'accès *e-banking* de la banque 14 (MPC 12-14-0003). « M. BB. » avait ensuite demandé à NNN. de lui confirmer divers éléments d'affichage sur la page web. « M. BB. » avait alors un visuel de l'écran de NNN. Il avait interpellé ce dernier sur la validation de paiements en suspens, ce sur quoi, NNN. avait expliqué à « M. BB. » que sa supérieure, OOO., devait valider les transactions. Parallèlement, « M. BB. » lui avait demandé d'afficher à l'écran la liste des collaborateurs ayant un droit de signature pour les paiements. Sur indications de « M. BB. », NNN. s'était ensuite muni de l'identificateur […]. Toujours sur instruction de « M. BB. » et sans saisir le sens de ces démarches, NNN. avait parcouru plusieurs menus *e-banking*, et introduit des données dictées par « M. BB. ». A la demande de « M. BB. », NNN. avait ensuite passé le combiné à OOO. (MPC 12-14-0004). Le 14 juin 2018, entre 15h00 et 16h00, « M. BB. »

avait recontacté NNN., l'informant que la migration se passait bien avant d'évoquer deux paiements dont le numéro de clearing manquait. A l'issue de la conversation, « M. BB. » avait encore indiqué à NNN. qu'il le rappellerait le lendemain matin (MPC 12-14-0005).

Q.2.5 Lors de son audition du 15 juin 2018 (MPC 05-09-0005 ss), OOO. a expliqué avoir été mise en contact avec un « M. BB. » de la banque 14, le 13 juin 2018, aux alentours de 16h40, par l'entremise de son collègue, NNN. OOO. s'était connectée à sa session *e-banking*, à la demande de « M. BB. » (MPC 05-09-0007). Ce dernier l'avait ensuite redirigée vers les paiements encore ouverts. Il lui avait après indiqué que la migration de la plateforme *e-banking* durerait 72 heures. Il lui avait toutefois précisé qu'en cas de paiement à effectuer, il lui suffirait de l'appeler pour qu'il lui donne un accès temporaire à la plateforme. OOO. avait alors confirmé à « M. BB. » qu'il n'y aurait pas nécessité de faire des paiements pendant la migration. Il avait alors requis qu'elle se reconnecte à la plateforme *e-banking*, ce qu'elle n'avait toutefois pas fait. Par la suite, « M. BB. » avait recontacté la société et signalé à OOO. des soi-disant erreurs sur deux des paiements fournisseurs préparés dans le fichier DTA et indiqué qu'il devait parler à NNN. (MPC 05-09-0008).

Q.2.6 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier la prise de contact avec O. (MPC 13-01-0097, 13-01-0101, 13-01-0192 et 13-01-0198). Lors de son audition du 28 octobre 2022, le prévenu a finalement admis être « M. BB. » qui avait contacté la société O. (MPC 13-01-0247 et 13-01-0264). Il a précisé se souvenir « avoir eu le trac », dans ce cas-là – O. étant une grande société – et que lui (et ses comparses) s'étaient dit qu'il devait y avoir beaucoup d'argent sur ses comptes (MPC 13-01-0264).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

R. M. (chiffre 1.3.14 de l'acte d'accusation)

R.1 <u>Des faits reprochés au prévenu</u>

R.1.1 A teneur de l'acte d'accusation, le 26 juin 2018, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté la société M. à VV. en se présentant sous le pseudonyme de « CC. » et en affirmant travailler pour la banque 14. Il a indiqué à QQQ., chef comptable de la société, qu'une migration du service *e-banking* devait être effectuée dans les jours qui suivaient et l'a prié d'introduire l'adresse URL « 14 » dans la barre adresse de son navigateur internet. Ce faisant, le prévenu a amené son interlocuteur à télécharger à son insu le logiciel de contrôle à distance NTRCloud. Le prévenu a ensuite demandé à QQQ. de se connecter à une session *e-banking* et a ainsi pu prendre

connaissance indument des données d'accès de ce dernier à son insu, notamment lorsque celui-ci a cliqué à sa demande sur la fonction faisant apparaître le mot de passe en clair. Le prévenu a encore prié QQQ. de collecter les mots de passe et identifiants des autres employés de la société ayant accès à l'*e-banking* et lui a fait s'identifier. Le prévenu a ensuite fait répéter à QQQ. les opérations mentionnées plus haut avec les accès du directeur financier, RRR.

R.1.2 Toujours selon l'acte d'accusation, au moyen des accès susmentionnés, obtenus illicitement, le prévenu a pu pénétrer sans droit dans le système informatique de M. les 26 et 28 juin 2018 et prendre connaissance illicitement de données de la société, en particulier des données bancaires et des accès *e-banking*. Il a également communiqué les accès ainsi obtenus aux autres auteurs, leur permettant de la sorte de pénétrer sans droit à plusieurs reprises entre le 26 et le 28 juin 2018 dans le système informatique de la société précitée et d'ouvrir des sessions *e-banking*, d'accéder aux comptes de cette dernière auprès de la banque 14 et d'ordonner les transferts suivants :

1) le 26 juin 2018 : EUR 89'328.- en faveur du compte 48 au nom de la société 34 auprès de la banque 20 (D), bloqué en Allemagne et retourné à la banque 14 ;

2) le 28 juin 2018 : EUR 97'000.- en faveur du compte 49 au nom de la société 35 auprès de la banque 21 à Bratislava (SK), transfert bloqué par la banque 14 avant son exécution.

R.2 Des moyens de preuve

R.2.1 Il ressort des documents bancaires produits par M. que sa relation auprès de la banque 14 a été débitée de EUR 89'328.- le 26 juin 2018 en faveur du compte n° 48 au nom de la société 34, logé auprès de la banque 20 (D) (MPC 10-02-0192). Ladite relation a en outre été débitée en faveur du compte de la société 35 auprès de la banque 21 à Bratislava (SK) (MPC 10-02-0194).

R.2.2 La PJF a procédé à une analyse forensique d'une copie miroir de l'ordinateur de QQQ. (MPC 10-02-0064). Il en ressort que le logiciel NTRCloud a été téléchargé et exécuté consécutivement à une visite du site tinyurl, le 26 juin 2018 à 9h30 et 13h29. Après le téléchargement de NTRCloud, une activité *e-banking* est enregistrée depuis l'appareil (MPC 10-02-0323 ss). Les adresses IP opérateur des connexions à distance NTRCloud correspondent à des adresses israéliennes provenant de la plage d'adresses IP 46 appartenant au provider société 24 (MPC 10-02-0325).

R.2.3 QQQ. a été auditionné le 28 juin 2018 et a, en substance, décrit les agissements tels que reprochés au prévenu (MPC 12-18-0001 ss). Il a ainsi expliqué que le 26 juin 2018, vers 11h30, l'auteur l'avait contacté depuis le raccordement 2, se présentant sous le nom de « CC. » du service *e-banking* de la banque 14. QQQ. avait, par le passé, déjà eu contact avec ledit interlocuteur, qui l'avait appelé au sujet d'une migration et de mise à jour de l'*e-banking*, dans les trois mois précédents. Lors de l'appel du 26 juin 2018, « CC. » avait commencé par poser à QQQ. quelques questions de satisfaction client, puis lui a annoncé qu'une migration ou mise à jour du système serait nécessaire dans les jours qui venaient mais qu'avant de la lancer, il fallait encore vérifier quelques points. « CC. » avait alors demandé à QQQ. de se connecter à internet et de taper dans la barre d'adresse un lien tinyurl.com. QQQ. avait effectué ces démarches puis avait cliqué sur le bouton « exécuter » s'affichant sur son écran. A la demande de « CC. », QQQ. s'était ensuite connecté à son *e-banking*. Toujours à la demande de « CC. », il avait alors cliqué sur le logo en forme d'œil apparaissant à côté du bouton login et était entré sur site. « CC. » avait ensuite posé plusieurs questions à QQQ. sur l'apparence du site sur son écran ainsi que sur les opérations bancaires effectuées par la société et les personnes habilitées à les exécuter (MPC 12-08-0003 s.). QQQ. lui avait répondu. « CC. » lui avait ensuite demandé de récupérer les mots de passe et les identifiants de ses collègues. Il lui avait fait s'identifier. Toujours à la demande de « CC. » QQQ. avait répété ces opérations avec les identifiants du Directeur financier, M. RRR., qui comme QQQ., était habilité à signer, collectivement à deux, pour la société. « CC. » avait encore informé QQQ. de l'impossibilité de se connecter à l'*e-banking* pendant la migration, et, sur sa proposition, avait accompagné QQQ. dans l'exécution des deux virements que ce dernier devait encore effectuer. « CC. » avait ensuite demandé à QQQ. de récupérer les identifiants de ses collègues de M.a., filiale suisse de M., située dans le même bâtiment. Un desdits collègues étant parti en pause, « CC. » avait rappelé QQQ. en début d'après-midi, vers 13h30 ou 14h. Toujours sur instructions de « CC. », QQQ. avait alors effectué la même procédure que le matin même, s'agissant cette fois de la relation M.a. Le 26 juin 2018 au soir, la banque informait le Directeur financier de la société d'un virement frauduleux opéré sur le compte de celle-ci, soit d'un versement de EUR 89'328.- sur le compte de la société 34 (MPC 12-18-0004). Le lendemain matin, 27 juin 2018, vers 9h00 « CC. » avait une fois de plus appelé QQQ., depuis le même raccordement 2 et lui avait demandé si tout allait bien (MPC 12-18-0004 s.). Par la suite, la banque a informé QQQ. qu'outre la transaction de EUR 89'328.-, un ordre de virement d'EUR 97'000.-, au débit de la relation de M., avait été bloqué. L'entité récipiendaire était la société 35 à Bratislava (SK) (MPC 12-18-0005 s.).

R.2.4 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier la prise de contact avec la société M. (MPC 13-01-0098 et 13-01-0197). Lors de son audition du 28 octobre 2022, le prévenu a finalement admis être « CC. » qui avait contacté la société M.a. (MPC 13-01-0247).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

S. P. (chiffre 1.3.15 de l'acte d'accusation)

S.1 Des faits reprochés au prévenu

S.1.1 A teneur de l'acte d'accusation, le 27 juin 2018, en fin d'après-midi, depuis un lieu en Israël qui n'a pu être déterminé précisément, l'un des auteurs non identifiés a appelé téléphoniquement la société P. à WW., se présentant sous le pseudonyme de « GG. » et affirmant travailler au service connectique de la banque 4. L'individu a indiqué qu'une mise à jour du système *e-banking* devait avoir lieu, laquelle entraînerait une coupure de ce service durant 48 à 72 heures. Il s'est successivement entretenu avec plusieurs employés, en particulier le comptable SSS. et la directrice financière TTT. au sujet du système *e-banking* et du paiement de factures en cours. Il a encore indiqué que l'un de ses collègues nommé « BB. » rappellerait le lendemain matin vers 11h pour leur communiquer « le numéro de migration ».

S.1.2 Le 28 juin 2018, vers 11h50, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a appelé SSS. sur sa ligne directe en se présentant sous le pseudonyme de « BB. », prétendument employé par la banque 4. Le prévenu a prié son interlocuteur d'ouvrir une nouvelle page internet à l'adresse URL « 15 », puis de cliquer sur la fonction « exécuter » qui s'affichait sur l'écran. Ce faisant, le prévenu a amené SSS. à télécharger à son insu le logiciel de contrôle à distance NTRCloud, lequel lui a permis d'accéder sans droit à l'ordinateur de ce dernier et, partant, au système informatique de la société susmentionnée. Le prévenu a ensuite prié SSS. d'ouvrir une session *e-banking* puis l'a dirigé vers l'onglet « paiements » dans l'interface de la session, avant de lui demander de cliquer sur l'onglet des paiements exécutés, prenant ainsi connaissance indument des données bancaires de la société à l'insu de son interlocuteur. Il a encore demandé à celui-ci de sortir de sa session, puis de se reconnecter et d'utiliser le clavier virtuel pour entrer son code personnel (NIP). En procédant de la sorte, le prévenu a également pris connaissance sans droit des données d'accès de SSS., sans que celui-ci n'en ait conscience. Il a ensuite annoncé à SSS. que la « migration » ne commencerait que le lundi suivant et qu'il le rappellerait à cette date.

S.2 Des moyens de preuve

S.2.1 La PJF a procédé à une analyse forensique de l'ordinateur de SSS. (MPC 10-02-0059 et 10-02-327 ss) et à celle de l'extrait du trafic réseau de P. en relation avec la plage d'adresses IP 46 (MPC 10-02-0060). Il en ressort que le 28 juin 2018, à 9h56, une connexion à distance NTRCloud a été établie avec l'appareil et qu'en suite, à 10h18, 8 paquets de données ont été capturés sur le pare-feu de P., après établissement de la connexion NTRCloud. L'adresse de destination IP était une adresse IP israélienne provenant d'une plage IP appartenant au provider israélien société 24.

S.2.2 Les mesures de surveillance ont permis d'intercepter un appel de « GG. » du 27 juin 2018, au cours duquel celui-ci qui annonce une migration *e-banking* et un appel de son collègue « BB. ». « GG. » se renseigne sur la satisfaction client, les processus bancaires de la société et les personnes habilitées à effectuer des transactions sur ses comptes. Il annonce que la migration va occasionner une coupure provisoire du système *e-banking* et s'enquiert des paiements en suspens (MPC 10-02-0086 ss ; rubrique 13 ID1000049471941).

S.2.3 L'enquête a aussi permis d'enregistrer la conversation du 28 juin 2018 entre SSS. et « BB. ». L'interlocuteur « BB. » se réfère à la discussion entre SSS. et « GG. ». Il s'assure que la société a d'ores et déjà pu effectuer les paiements urgents et lui demande de vérifier que ses collègues – qui nécessiteront leur propre numéro de migration – ne partent pas en pause de midi. Il se réfère aux avantages de la migration et s'informe sur les habitudes de paiement de la société et les programmes utilisés. Il demande ensuite à SSS. d'ouvrir une page internet, lui indique une adresse url tinyurl, de cliquer sur le bouton « exécuter », soi-disant pour lui donner un numéro de migration, et le guide sur l'*e-banking*. Sur instruction de « BB. », SSS. affiche la page des paiements exécutés et les classe par montants décroissants, puis se déconnecte de sa session l'*e-banking*. A la demande de « BB. », il se reconnecte à l'*e-banking* et fait apparaître le clavier numérique en introduisant son mot de passe avec le curseur en laissant trois secondes entre chaque clic. Il l'informe que l'*e-banking* sera interrompu et lui demande s'il doit encore effectuer des paiements. Ensuite de certaines difficultés techniques, l'interlocuteur annonce que la migration va finalement débuter lundi et demande à SSS. de veiller à bien effectuer tous ses paiements d'ici-là (MPC 10-02-0094 ss, rubrique 13, ID1000049521298).

S.2.4 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier la prise de contact avec P. (MPC 13-01-0072 et 13-01-0098), y compris lorsque confronté à l'enregistrement audio du 28 juin 2018, ID 1000049521298 (MPC 13-01-0177), soutenant alors ne pas reconnaître les voix sur l'enregistrement. Lors de son audition du 28 octobre 2022, le prévenu a admis être « BB. » qui avait contacté la société P. (MPC 13-01-0247).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

T. Société 4 (chiffre 1.3.16 de l'acte d'accusation)

T.1 Des faits reprochés au prévenu

T.1.1 A teneur de l'acte d'accusation, le 5 juillet 2018, à 11h21, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté la société 4 à XX. en se présentant sous le pseudonyme de « CC. » et en affirmant travailler pour la banque 14. Il a demandé à pouvoir s'entretenir avec un/e collaborateur/trice du service de la comptabilité ou en charge de la saisie des paiements, mais son appel n'a pu être transféré.

T.1.2 Le prévenu a rappelé la société le même jour à 12h16 et a été mis en contact avec AAAA., employée du service de comptabilité qu'il a convaincue d'introduire l'adresse URL « www.37 » dans la barre adresse de son navigateur. Le prévenu a agi ainsi dans le dessein d'amener son interlocutrice à télécharger le logiciel de contrôle à distance NTRCloud et de lui permettre de prendre connaissance des données d'accès *e-banking* et des données bancaires de la société, ainsi que de permettre aux autres auteurs de transférer indument des fonds par le débit des comptes de cette société en leur faveur. Il n'est toutefois pas parvenu à accéder à distance à l'ordinateur de son interlocutrice en raison du paramétrage de sécurité de la société précitée.

T.2 Des moyens de preuve

T.2.1 La conversation du 5 juillet 2018 entre « CC. » et AAAA. a été interceptée (MPC 10-02-0208). Il en ressort que « CC. » procède par le mode opératoire habituel et demande à son interlocutrice de taper une adresse URL tinyurl.com dans sa barre de recherche, laquelle s'exécute. La connexion ne peut toutefois être établie, en raison du paramétrage technique lié à la sécurité informatique de la société (MPC 10-02-0208 et 10-02-0252 ss ; rubrique 10-08).

T.2.2 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier la prise de contact avec la société 4 (MPC 13-01-0103). Lors de son audition du 28 octobre 2022, le prévenu a finalement décidé de s'expliquer (MPC 13-01-0236), précisant être impliqué dans les cas perpétrés au mois de mai, juin, juillet et août 2018 (MPC 13-01-0243). Sur présentation des tentatives répertoriées pour la période entre juin et octobre 2018, le prévenu a confirmé être l'auteur des appels correspondant aux pseudonymes « BB. » et « CC. » notamment, dont des appels à la société 4 des 4 et 5 juillet 2018 et l'a confirmé le 30 novembre 2022 (MPC 13-01-0271 ; 13-01-0283 ss et 13-01-0298 s.).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

U. Société 5 (chiffre 1.3.17 de l'acte d'accusation)

U.1 Des faits reprochés au prévenu

U.1.1 A teneur de l'acte d'accusation, le 10 juillet 2018, à 11h07, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté la société 5 en se présentant sous le pseudonyme de « CC. ». Il a indiqué à BBBB., employée en charge de la saisie des paiements, qu'il travaillait avec la banque 14 et qu'en raison d'un changement de protocole, une migration du système *e-banking* était nécessaire et risquait d'occasionner une interruption de 48 à 72 heures. Sous prétexte de lui communiquer son numéro de migration, il lui a demandé d'ouvrir une page internet et lui a dicté l'adresse « 16 », afin de lui faire télécharger à son insu le logiciel de contrôle à distance NTRCloud, sans succès toutefois, la conversation ayant été interrompue pour un motif indéterminé.

U.1.2 Aucun transfert n'a pu être ordonné dans ce cas.

U.1.3 Toujours selon l'acte d'accusation, le prévenu a ainsi tenté d'accéder indument au système informatique de la société susmentionnée dans le dessein de prendre connaissance sans droit des données de la société et de permettre aux autres auteurs de transférer indument des fonds par le débit des comptes de cette société en leur faveur.

U.2 Des moyens de preuve

U.2.1 La surveillance téléphonique sur le raccordement 2 a permis de constater qu'en date du 10 juillet 2018, l'individu se présentant comme « CC. » de la banque 4 a contacté le numéro 50 de la société 5 et qu'il a pris contact avec BBBB. Il lui a ensuite posé plusieurs questions sur les personnes ayant accès à quels comptes de la société. BBBB. répondant qu'elle n'a accès qu'à la relation de la banque 14, « CC. » indique qu'il appelle (en fait) de la banque 14. Il lui demande ensuite si elle a constaté des ralentissements sur le portail, l'informe que la migration va prendre jusqu'à 48h ou 72h et lui pose des questions quant aux habitudes de paiement de la société. Il lui dicte ensuite l'adresse « 16 » et la prie de cliquer sur « exécuter » (MPC 10-02-0209 et 10-02-0366, société 5 ID 1000050204298 ; rubrique 10-08).

U.2.2 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier d'avoir contacté la société 5 (MPC 13-01-0104). Lors de son audition du 28 octobre 2022, le prévenu a finalement décidé de s'expliquer (MPC 13-01-0236), précisant être impliqué dans les cas perpétrés au mois de mai, juin, juillet

et août 2018 (MPC 13-01-0243). Sur présentation des tentatives répertoriées pour la période entre juin et octobre 2018, le prévenu a confirmé être l'auteur des appels correspondant aux pseudonymes « BB. », « CC. » et « DD. », dont des appels à la société 5 du 10 juillet 2018 et l'a confirmé le 30 novembre 2022. (MPC 13-01-0271 ; 13-01-0285 ss et 13-01-0298 s.).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

V. Société 6 (chiffre 1.3.18 de l'acte d'accusation)

V.1 Des faits reprochés au prévenu

V.1.1 A teneur de l'acte d'accusation, le 18 juillet 2018 à 11h09, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté la société 6 à YY., en se présentant sous le pseudonyme de « CC. » et en affirmant travailler pour la banque 14. Mis en contact avec CCCC., employée en charge des paiements en ligne, le prévenu lui a expliqué qu'une migration du système *e-banking* devait occasionner une interruption de sa disponibilité de 48 à 72 heures. Sous prétexte de lui communiquer son numéro de migration, le prévenu lui a demandé d'ouvrir une page internet et lui a dicté l'adresse « www.38 » dans le but de lui faire télécharger le logiciel de contrôle à distance NTRCloud. La page internet ne s'affichant pas, le prévenu lui a dicté d'autres adresses, à savoir «17», «18», «19» et finalement «20», sans plus de succès. Il a finalement été convenu que CCCC. rappellerait son interlocuteur dans l'après-midi, ce qu'elle n'a pas fait.

V.1.2 Aucun transfert n'a pu être ordonné dans ce cas.

V.1.3 Toujours à teneur de l'acte d'accusation, le prévenu a ainsi tenté d'accéder indument au système informatique de la société 6 dans le dessein de prendre connaissance sans droit des données de la société et de permettre aux autres auteurs de transférer indument des fonds par le débit des comptes de cette société en leur faveur.

V.2 Des moyens de preuve

V.2.1 La surveillance téléphonique sur le raccordement 2 a permis de constater qu'en date du 18 juillet 2018, l'individu se présentant comme « CC. » a contacté le numéro 51 de la société 6. Mis en relation avec CCCC., « CC. » lui demande si le système a subi des ralentissements, l'interroge sur les habitudes de paiement de la société et les paiements devant être effectués. Il lui fait taper plusieurs adresses tinyurl.com (MPC 10-02-0203 et 10-02-0366 et 10-02-374 ; société 6 ID 1000050633049 ; rubrique 18.08).

V.2.2 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier la prise de contact avec la société 6 (MPC 13-01-0104). Lors de son audition du 28 octobre 2022, le prévenu a finalement décidé de s'expliquer (MPC 13-01-0236), précisant être impliqué dans les cas perpétrés au mois de mai, juin, juillet et août 2018 (MPC 13-01-0243). Sur présentation des tentatives répertoriées pour la période entre juin et octobre 2018, le prévenu a confirmé être l'auteur des appels correspondant aux pseudonymes « BB. », « CC. » et « DD. », dont l'appel à la société 6 du 18 juillet 2018 et l'a confirmé le 30 novembre 2022 (MPC 13-01-0271 ; 13-01-0285 ss et 13-01-0298 s.).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

W. Société 38 (chiffre 1.3.19 de l'acte d'accusation)

W.1 Des faits reprochés au prévenu

W.1.1 A teneur de l'acte d'accusation, le 18 juillet 2018 à 12h13, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté la société 38 à Genève en se présentant sous le pseudonyme de « CC. » et en affirmant travailler pour la banque 22. Toujours sous le prétexte d'une prétendue migration du système *e-banking*, le prévenu a convaincu l'un des employés chargés des paiements d'introduire les adresses URL «21», «22» et «23» dans son navigateur internet afin de lui faire télécharger le logiciel de contrôle à distance NTRCloud. Ne parvenant pas à ses fins, le prévenu a alors demandé à son interlocuteur de télécharger le logiciel de contrôle à distance TeamViewer, toujours sans succès. Il l'a alors prié d'introduire l'adresse URL «24», ce qui a permis à son interlocuteur de télécharger le logiciel précité, sans toutefois que la connexion avec le prévenu ne puisse se faire.

W.1.2 Le 19 juillet, à 10h59, le prévenu a rappelé la société susmentionnée sous le même pseudonyme, tentant vainement de convaincre le responsable IT d'autoriser le collaborateur contacté la veille à télécharger le programme NTRCloud.

W.1.3 Le prévenu a ainsi tenté d'accéder indument au système informatique de la société 38 dans le dessein de prendre connaissance sans droit des données de la société et de permettre aux autres auteurs de transférer indument des fonds par le débit des comptes de celle-ci en leur faveur.

W.2 Des moyens de preuve

W.2.1 La surveillance téléphonique sur le raccordement 2 a permis de constater qu'en date du 18 juillet 2018, l'individu se présentant comme « CC. » a contacté la société 38. Il interroge son interlocuteur sur la nécessité de procéder à des versements le jour-même et le nombre de personnes accédant au portail. Il demande ensuite à son interlocuteur de taper une adresse URL tinyurl.com pour lui donner son numéro de migration. En raison de problèmes techniques, « CC. » demande ensuite à son interlocuteur de taper une nouvelle adresse tinyurl, ce qui provoque le téléchargement du logiciel DDDD., qui n'aboutit pas non plus (MPC 10-02-0212). Le lendemain, à 10h59 « CC. » appelle un responsable IT de la société, évoque l'impossibilité pour le collaborateur contacté la veille de télécharger l'outil permettant d'obtenir son numéro de migration. « CC. » demande à son interlocuteur d'autoriser le collaborateur contacté la veille à télécharger le programme NTRCloud, excipant d'une urgence à démarrer la migration le matin même. Le responsable IT met un terme à la conversation en demandant que « CC. » lui envoie un courriel (MPC 10-02-0213 et 10-02-0263 ss, rubrique 10-08, société 38 ID 1000050635382).

W.2.2 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier la prise de contact avec la société 38 (MPC 13-01-0105 et 13-01-0148 s.). Lors de son audition du 28 octobre 2022, le prévenu a finalement décidé de s'expliquer (MPC 13-01-0236), précisant être impliqué dans les cas perpétrés au mois de mai, juin, juillet et août 2018 (MPC 13-01-0243). Sur présentation des tentatives répertoriées pour la période entre juin et octobre 2018, le prévenu a confirmé être l'auteur des appels correspondant aux pseudonymes « BB. », « CC. » et « DD. », dont l'appel à la société 38 du 18 juillet 2018 et l'a confirmé le 30 novembre 2022 (MPC 13-01-0271 ; 13-01-0296 et 13-01-0298 s.).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

X. Société 7 (chiffre 1.3.20 de l'acte d'accusation)

X.1 Des faits reprochés au prévenu

X.1.1 A teneur de l'acte d'accusation, le 23 juillet 2018 à 12h01, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté la société 7 à Genève en se présentant sous le pseudonyme de « CC. » et en affirmant travailler pour la banque 4, dans un premier temps. Expliquant qu'une mise à jour du système *e-banking* allait prochainement entraîner une interruption de l'accès au portail durant 48 à 72 heures, il a convaincu EEEE., employée de la société chargée de saisir les paiements, d'introduire dans la barre adresse de son navigateur l'adresse « 25 ». EEEE. l'ayant interrompu pour lui indiquer que la

société ne travaillait pas avec la banque 4, mais avec la banque 23 le prévenu a réussi à la convaincre qu'elle avait mal compris et qu'il travaillait bien pour cette dernière banque. Il l'a ensuite priée d'ouvrir une nouvelle page internet et lui a dicté l'adresse « 26 », lui faisant ainsi télécharger à son insu le logiciel de contrôle à distance NTRCloud. Il lui a ensuite demandé de cliquer sur la fonction « exécuter » et lui a communiqué un soi-disant numéro de migration à introduire – en réalité le code lui permettant d'activer le contrôle à distance et d'accéder ainsi indument à l'ordinateur de son interlocutrice. Le prévenu a alors prié EEEE. d'ouvrir une session *e-banking* et a procédé avec elle à diverses vérifications sur les paramètres du système *e-banking*, avant de lui demander de se déconnecter. Il lui a expliqué qu'il reprendrait contact avec les responsables financiers autorisés à valider les ordres de paiements, absents à ce moment.

X.1.2 Il n'a toutefois pas recontacté la société et aucun transfert n'a été ordonné par les autres auteurs par le débit des comptes de la société 7.

X.1.3 Le prévenu a ainsi tenté d'accéder indument au système informatique de la société 7 dans le dessein de prendre connaissance sans droit des données de la société et de permettre aux autres auteurs de transférer indument des fonds par le débit des comptes de cette société en leur faveur.

X.2 Des moyens de preuve

X.2.1 La surveillance téléphonique sur le raccordement 2 a permis de constater qu'un individu se présentant comme « CC. » de la banque 4 a contacté EEEE. de la société 7, le 23 juillet 2018. Après lui avoir demandé si elle avait observé des ralentissements, il lui pose des questions quant aux habitudes de paiement de la société. EEEE. relevant que la société n'a pas de relation auprès de la banque 4, il prétend appeler depuis la banque 23 et arrive à convaincre son interlocutrice qu'il s'agit d'une méprise. Ensuite, « CC. » donne à EEEE. un « numéro de migration » puis lui dicte une adresse tinyurl.com et lui demande de se connecter au portail *e-banking*. Une fois la connexion établie, « CC. » guide EEEE. sur sa session *e-banking* et lui pose des questions quant aux paiements devant être effectués prochainement et aux droits de signature sur le compte. Il lui indique qu'il la rappellera dans l'après-midi (MPC 10-02-0214, 10-02-0374 et 10-02-0366 ID 1000050869022 et 100050869572).

X.2.2 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier l'appel à la société 7 (MPC 13-01-0106 et 13-01-0150). Le 10 novembre 2022, sur présentation des tentatives répertoriées pour la période entre juin et octobre 2018, le prévenu a confirmé être l'auteur des appels correspondant aux pseudonymes « BB. », « CC. » et « DD. », dont l'appel à la société 7 du 23 juillet 2018 (MPC 13-01-0271 et 13-01-0287). Il l'a confirmé à nouveau le 30 novembre 2022 (MPC 13-01-0297 et 13-01-0298 s.).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

Y. Société 8 (chiffre 1.3.21 de l'acte d'accusation)

Y.1 Des faits reprochés au prévenu

Y.1.1 A teneur de l'acte d'accusation, le 24 juillet 2018 à 11h14, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté la société 8 à Genève en se présentant sous le pseudonyme de « CC. » et en affirmant travailler pour la banque 14. Il a ensuite pu convaincre Mme FFFF., employée en charge des paiements d'introduire l'adresse URL suivante dans son navigateur : « 27 », lui faisant ainsi télécharger le logiciel de contrôle à distance NTRCloud dans le but d'accéder au système informatique de la société susmentionnée et de prendre connaissance des données de celle-ci. Il l'a ensuite priée de se connecter sur la plateforme *e-banking* de la banque 14 et de lui confirmer différentes informations sur cette plateforme. Constatant qu'il s'agissait d'une société israélienne, le prévenu a toutefois finalement renoncé à poursuivre son activité délictueuse et a indiqué à son interlocutrice que la version *e-banking* était à jour et ne nécessitait finalement aucune migration.

Y.1.2 Le prévenu a ainsi tenté d'accéder indument au système informatique de la société susmentionnée dans le dessein de prendre connaissance sans droit des données de la société et de permettre aux autres auteurs de transférer indument des fonds par le débit des comptes de cette société en leur faveur.

Y.2 Des moyens de preuve

Y.2.1 La surveillance du raccordement 2 a permis d'enregistrer une prise de contact de « CC. » avec la société 8 sur son numéro 52, le 24 juillet 2018. Lors de ladite communication, en anglais, « CC. » évoque une « migration », pose à son interlocutrice quelques questions quant à sa satisfaction d'utilisateur et évoque une interruption de service d'une durée de 48h à 72h. Il la convainc de taper l'adresse URL 27 dans sa barre de recherche. Cette démarche aboutit, « CC. » l'invite à exécuter le logiciel NTR et prendre note du « numéro de migration ». Il l'accompagne dans sa navigation sur la page *e-banking*, l'invitant à afficher les transactions effectuées et des données d'accès. Après avoir demandé à son interlocutrice son nom (FFFF.) et avoir obtenu de celle-ci la confirmation que la société est israélienne, « CC. » fait marche arrière et informe son interlocutrice que la migration n'est plus nécessaire car elle dispose de la dernière version. « CC. » s'adresse ensuite à une tierce personne en arrière-fond et en français : « Nan, j'leur dis pas… euh banque 14…un million, OK ! » puis « Nan, j'leur dis pas, j'le fais pas… ça pue ! ». « CC. » conseille ensuite à son interlocutrice d'être méfiante car les entreprises peuvent être victimes de nombreuses escroqueries. Dans ce contexte, « CC. » fait notamment de la prévention contre les

escroqueries dites « au président ». « CC. » indique par la suite parler un peu l'hébreu, puis échange plusieurs mots dans cette langue avec son interlocutrice (MPC 10-02-0214 s. ; rubrique 10-08 société 8 enregistrement ID 1000050916906).

Y.2.2 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier toute implication dans la prise de contact avec la société 8, ce y compris après avoir été confronté à l'enregistrement de la conversation téléphonique, prétendant que celle-ci ne lui inspirait rien et indiquant ne comprendre que peu l'anglais mais avoir saisi les mots « fraud » et « careful » (MPC 13-01-0106 s. et 13-01-0151). Lors de son audition du 28 octobre 2022, le prévenu a finalement décidé de s'expliquer (MPC 13-01-0236), précisant être impliqué dans les cas perpétrés au mois de mai, juin, juillet et août 2018 (13-01-0243). Le 10 novembre 2022, sur présentation des tentatives répertoriées pour la période entre juin et octobre 2018, le prévenu a confirmé être l'auteur des appels correspondant aux pseudonymes « BB. », « CC. » et « DD. », dont l'appel à la société 8 du 23 juillet 2018 (MPC 13-01-0271 et 13-01-0288). Il l'a confirmé à nouveau le 30 novembre 2022 (MPC 13-01-0297 et 13-01-0298 s.).

Aux débats, A. a confirmé ses aveux (SK 37.731.014). Il a précisé avoir interrompu le cas sur signe de la main de « FF. » (SK 37.731.026).

Z. Société 39 (chiffre 1.3.22 de l'acte d'accusation)

Z.1 <u>Des faits reprochés au prévenu</u>

Z.1.1 A teneur de l'acte d'accusation, le 30 juillet 2018, à 11h25, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté la société 39 à Genève en se présentant sous le pseudonyme de « CC. » et en affirmant travailler pour la banque, sans préciser laquelle. Il a été mis en contact avec GGGG., employé de la société précitée, à qui il a expliqué qu'en raison de changements de protocoles et de nouveaux modules, le portail *e-banking* devait être interrompu durant 48 à 72 heures. Le prévenu a ensuite prié son interlocuteur d'ouvrir une page sur son navigateur internet et d'introduire l'adresse « 28 », dans le but de lui faire télécharger à son insu le logiciel de contrôle à distance DDDD. Aucune page internet ne s'affichant sur l'écran de GGGG., le prévenu lui a alors demandé de répéter l'exercice avec les adresses « 29 », puis « 30 » et « 31 », toujours sans parvenir à faire ouvrir la page internet voulue. Il a alors été mis en contact par son interlocuteur à sa demande avec un employé du service informatique qui a compris que le prévenu tentait de se faire faussement passer pour un représentant de la banque 24 et a mis fin à la conversation.

Z.1.2 Le prévenu a ainsi tenté d'accéder indument au système informatique de la société 39 dans le dessein de prendre connaissance sans droit des données de la société et de permettre aux autres auteurs de transférer indument des fonds par le débit des comptes de celle-ci en leur faveur.

Z.2 Des moyens de preuve

Z.2.1 La surveillance du raccordement 2 a permis d'enregistrer l'appel de « CC. » à la société 39 du 30 juillet 2018. Lors dudit appel, « CC. » informe son interlocuteur, GGGG., d'une soi-disant migration, de nouveaux modules d'incompatibilité et demande à GGGG. s'il a remarqué des ralentissements. Il évoque une interruption du portail entre 48 et 72 heures. « CC. » se renseigne ensuite sur la nécessité pour GGGG. d'effectuer des paiements et le type de ceux-ci, ainsi que les pays des comptes récipiendaires. Ensuite, « CC. » demande à son interlocuteur de taper l'adresse 28 dans sa barre de recherche. La page ne s'affichant pas chez GGGG., « CC. » l'instruit de taper l'adresse « 29 » et de cliquer sur le bouton « exécuter ». La page ne s'affichant toujours pas, « CC. » demande à son interlocuteur d'essayer avec d'autres liens qu'il lui dicte. Les démarches n'aboutissant pas, « CC. » demande à ce qu'un collaborateur de l'informatique vienne aider GGGG. à son poste. Le collaborateur informatique pose des questions à « CC. », en suite de quoi la conversation prend fin (MPC 10-02-0217 s. et 10-02-0276 ss ; rubrique 10-08 société 39 ID1000051159750).

Z.2.2 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier toute implication dans la prise de contact avec la société 39 (MPC 13-01-0108 et 13-01-0154). Lors de son audition du 28 octobre 2022, le prévenu a finalement décidé de s'expliquer (MPC 13-01-0236), précisant être impliqué dans les cas perpétrés au mois de mai, juin, juillet et août 2018 (MPC 13-01-0243). Le 10 novembre 2022, sur présentation des tentatives répertoriées pour la période entre juin et octobre 2018, le prévenu a confirmé être l'auteur des appels correspondant aux pseudonymes « BB. », « CC. » et « DD. », dont l'appel à la société 39 du 23 juillet 2018 (MPC 13-01-0271 et 13-01-0289). Il l'a confirmé à nouveau le 30 novembre 2022 (MPC 13-01-0297 ss).

Aux débats, A. a confirmé ses aveux (SK 37.731.014).

AA. J. (chiffre 1.3.23 de l'acte d'accusation)

AA.1 Des faits reprochés au prévenu

AA.1.1 A teneur de l'acte d'accusation, le 21 décembre 2016, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté la société J. à W. en se présentant sous le pseudonyme de « BB. » et en affirmant travailler pour la banque 14. Prétextant une migration du système *e-banking*, le prévenu a convaincu le responsable des finances d'introduire l'adresse URL « http://32 », afin de l'amener à télécharger à son insu un logiciel de contrôle à distance dans le but de prendre connaissance des données de la société susmentionnée. Son interlocuteur s'est toutefois méfié et a mis un terme à la conversation téléphonique, avant d'éteindre le système informatique et d'aviser les responsables de la société. Aucun transfert de fonds n'a pu être ordonné au préjudice de la société susmentionnée.

AA.1.2 Toujours à teneur de l'acte d'accusation, le prévenu a ainsi tenté d'accéder indument au système informatique de la société J. dans le dessein de prendre connaissance sans droit des données de la société et de permettre aux autres auteurs de transférer indument des fonds par le débit des comptes de celle-ci en leur faveur.

AA.2 Des moyens de preuve

AA.2.1 Le 21 décembre 2016, J. dénonçait à la police avoir été contacté via le numéro 17 par un certain « BB. », et décrivant en substance le déroulement des faits tels que reprochés au prévenu (MPC 05-05-0024).

Le raccordement utilisé par « BB. » pour contacter la société J. (17) est celui que le prévenu a utilisé pour contacter les sociétés G.a., aujourd'hui G., le 22 décembre 2016 (MPC 05-12-0018), H. (MPC 05-05-0029) et I. (MPC 05-02-0045) le 4 janvier 2017, K. le 9 janvier 2017 (MPC 05-02-0050) et B. le 16 janvier 2017 (MPC 05-00-0017).

AA.2.2 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier toute implication dans la prise de contact avec J. (MPC 13-01-0090 et 13-01-0115). Lors de son audition du 28 octobre 2022, le prévenu a finalement décidé de s'expliquer (MPC 13-01-0236) et a admis plusieurs cas. Il a toutefois maintenu ne pas être impliqué dans celui concernant J., excluant celui-ci car il serait selon lui antérieur à la première société dont il avait obtenu les identifiants *e-banking*, G.a., aujourd'hui G. (MPC 13-01-0241 et 13-01-0248), soit le 22 décembre 2016. Il a maintenu ses dénégations lors de son audition du 10 novembre 2022 (13-01-0273 s.), ainsi que celle du 30 novembre 2022 (13-01-0307 s.). Il faut toutefois relever que le prévenu a indiqué penser avoir lui-même effectué la première

phase de collecte d'informations dans le cas G., avant d'effectuer la deuxième phase de prise de contact en vue d'obtenir les accès (MPC 13-01-0258).

Par-devant la Cour de céans, le prévenu a maintenu ne pas être impliqué dans le cas J., au motif qu'il est antérieur à celui de G., son premier cas (SK 37.731.026).

BB. Société 9 (chiffre 1.3.24 de l'acte d'accusation)

BB.1 Des faits reprochés au prévenu

BB.1.1 A teneur de l'acte d'accusation, le 29 novembre 2017, entre 11h30 et 12h, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté la société 9 à Genève (aujourd'hui société 9.a.). Mis en contact avec le comptable de la société, HHHH., il s'est présenté sous le pseudonyme de « JJ. », affirmant travailler au service informatique de la banque 25. Prétextant une migration du système *e-banking*, il a posé plusieurs questions à son interlocuteur sur l'utilisation de l'*e-banking* dans la société, puis lui a dicté l'adresse URL « http://www.33 », l'amenant ainsi à télécharger à son insu le programme de contrôle à distance NTRCloud.

BB.1.2 Au moyen de ce logiciel, le prévenu a pu accéder indument au système informatique de la société 9 et prendre connaissance de données de ladite société. Il a en outre remis ces accès aux autres auteurs, leur permettant de se connecter, le 29 novembre 2017 entre 10h47 et 10h51, depuis un endroit non déterminé en Israël, au poste du comptable et d'accéder ainsi indument au système informatique de la société 9. Les auteurs ont ainsi pu prendre connaissance des données spécialement protégées de la société susmentionnée.

BB.1.3 Le prévenu a ensuite prié HHHH. de se connecter sur la plateforme *e-banking* de la banque 25, mais celui-ci ne s'est pas exécuté en raison de la méfiance que lui inspirait le prévenu. L'ayant mis en attente pour se renseigner sur la provenance de l'appel, le comptable a ensuite constaté que son interlocuteur avait raccroché.

BB.2 Des moyens de preuve

BB.2.1 La PJF a procédé à une analyse forensique d'une copie miroir de l'ordinateur de HHHH. Il en ressort que le 29 novembre 2017, à 10h47 l'appareil a téléchargé le logiciel NTRCould, qui, de manière coïncidente, a été exécuté, connectant à l'ordinateur de HHHH. l'appareil avec IP 53, laquelle correspond à une adresse IP israélienne de la plage d'adresses IP 46 appartenant au provider israélien « société 24 » (MPC 10-02-0305 s.)

BB.2.2 « M. JJ. » a contacté la société 9 en utilisant le raccordement 6 (MPC 12-04-0004 et 12-04-0007), soit le même que celui utilisé par le prévenu le 7 décembre 2017 pour le cas R. (MPC 05-04-0001 s.).

Le pseudonyme « JJ. » est proche, respectivement phonétiquement identique à celui de « KK. », utilisé pour le cas de la société 3, reconnu par le prévenu (MPC 13-01-0274). Dans le cas de la société 3, les dénommés « KKKK. », « KK. » et « BB. » avaient, successivement, contacté l'entreprise. Au contraire de « KKKK. » et « BB. », « KK. » n'appelait pas à l'aide d'un raccordement suisse mais depuis le numéro +54 (MPC 12-01-0003).

BB.2.3 Entendu le 27 décembre 2017 (MPC 12-04-0001 ss), HHHH. a expliqué qu'un certain « M. JJ. », prétendument du service informatique de la banque 25, l'avait contacté le 29 novembre 2017. Après avoir évoqué une migration, « M. JJ. » s'était enquis de la satisfaction client de HHHH., lui avait posé des questions détournées sur les droits d'accès au portail *e-banking* de la société, ainsi que des questions quant aux habitudes bancaires de celle-ci (MPC 12-04-0003). « M. JJ. » avait ensuite indiqué à HHHH. – qui devait partir en pause de midi – que le processus irait très vite. Il lui avait dicté le lien « 33 », lui avait demandé de cliquer sur « exécuter », puis de se connecter au portail *e-banking* (MPC 12-04-0003 s.). HHHH. ayant quelques soupçons, il avait fermé la page créée par le clic « exécuter », ce sur quoi « M. JJ. » lui avait demandé pourquoi il avait agi de la sorte (MPC 12-04-0004).

BB.2.4 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier toute implication dans la prise de contact avec la société 9 (MPC 13-01-0093 et 13-01-0123). Lors de son audition du 28 octobre 2022, le prévenu a finalement décidé de s'expliquer (MPC 13-01-0236 et 13-01-0198) et a admis plusieurs cas. Il a toutefois maintenu ne pas être impliqué dans celui concernant la société 9 (MPC 13-01-0248). Lors de son audition du 10 novembre 2022, il a expliqué exclure ce cas en raison du pseudo utilisé, « M. JJ. » (MPC 13-01-0274).

Par-devant la Cour de céans, le prévenu a maintenu ses dénégations (SK 37.731.026 s.)

CC. Q. (chiffre 1.3.25 de l'acte d'accusation)

CC.1 <u>Des faits reprochés au prévenu</u>

CC.1.1 A teneur de l'acte d'accusation, le 24 mai 2018, vers 15h15, à Netanya (IL), depuis un lieu qui n'a pu être déterminé précisément, le prévenu a contacté la société Q. à Lausanne sous le pseudonyme « II.a. ». Affirmant travailler au service technique de la banque 25, il a prié IIII., employée de la société précitée

en charge des paiements en ligne, d'ouvrir l'e-mail qu'il lui avait envoyé et de cliquer sur le lien qu'il contenait. Ce lien ne fonctionnant pas, le prévenu a demandé à son interlocutrice d'ouvrir une page internet à l'adresse URL « www.34 », dans le dessein de lui faire télécharger un logiciel de contrôle à distance à son insu, mais sans plus de succès. Le prévenu lui a alors indiqué qu'il la rappellerait plus tard, mais IIII. a contacté la police, mettant fin à l'échange.

CC.1.2 Le prévenu a ainsi tenté d'accéder indument au système informatique de la société Q. dans le dessein de prendre connaissance sans droit des données de la société et de permettre aux autres auteurs de transférer indument des fonds par le débit des comptes de celle-ci en leur faveur.

CC.2 Des moyens de preuve

CC.2.1 A l'appui de sa plainte, la société Q. a produit une copie du courriel adressé le 24 mai 2018 par « II.a. », à IIII., depuis l'adresse « II.a.@cyberservices.com », lui demandant une confirmation de son identité par retour de courriel et comprenant le lien raccourci qu'elle devait utiliser pour la soi-disant mise à jour (MPC 10-02-0158).

CC.2.2 Entendue le 28 mai 2018 (MPC 12-08-0001 ss), IIII. a en substance décrit le comportement de son interlocuteur tel que reproché au prévenu. Elle a ainsi expliqué que le 24 mai 2018, elle avait reçu un appel téléphonique dont l'appelant était masqué. Son interlocuteur s'était annoncé comme étant « II.a. » du service technique de la banque 25. « II.a. » lui avait demandé confirmation que c'était bien elle qui s'occupait des paiements en ligne. « II.a. » lui avait ensuite envoyé un e-mail, lui demandant d'y répondre, pour des questions de sécurité, selon ses dires (MPC 12-08-0002). IIII. s'étant exécutée, « II.a. » lui avait demandé si elle avait constaté des ralentissements sur le portail *e-banking*. « II.a. » lui avait parlé d'une mise à jour et lui avait demandé de cliquer sur le lien hypertexte figurant dans le mail qu'il lui avait envoyé. Un grand carré rouge et un message d'erreur s'affichant à l'écran de IIII., « II.a. » l'avait priée de répéter la manipulation. Celle-ci ayant également débouché sur le message d'erreur, « II.a. » avait alors prié IIII. d'ouvrir son navigateur internet, puis lui avait dicté l'adresse, 34 (MPC 12-08-0003). Conformément aux instructions de « II.a. », IIII. avait alors essayé de cliquer sur un bouton rouge apparaissant à l'écran, sans succès. « II.a. » s'était agacé, lui indiquant qu'il la rappellerait dans 5 minutes. Entretemps mise en garde par un collègue et après un contact avec la banque, IIII. avait ensuite refusé plusieurs appels masqués, provenant a priori de « II.a. » (MPC 12-08-0004).

CC.2.3 Le 24 mai 2018, à 8h53 – soit quelques heures avant la prise de contact de « II.a. » – une collègue d'IIII., JJJJ., a communiqué les coordonnées de deux comptes bancaires de la société Q. à l'adresse « HH.a.@gmail.com » (MPC 10-07-0077). Le courriel fait référence à une demande idoine de l'interlocuteur, sans

qu'il en ressorte si la demande a été formée par courriel ou lors d'un entretien téléphonique.

A teneur des résultats d'enquête, l'adresse « HH.a.@gmail.com » a été utilisée pour recueillir de 16 sociétés suisses leurs coordonnées bancaires, dont la société Q., et que ces sociétés ont ensuite fait l'objet de tentatives de fraude. Les 15 autres sociétés ne font pas l'objet des cas reprochés au prévenu aux termes de l'acte d'accusation (MPC 10-07-0072 ss).

CC.2.4 Dans un premier temps, le prévenu a, à réitérées reprises, nié catégoriquement toute implication dans les faits objet de la procédure, en particulier toute implication dans la prise de contact avec la société Q. (MPC 13-01-0096 et 13-01-0130). Lors de son audition du 28 octobre 2022, le prévenu a finalement décidé de s'expliquer (MPC 13-01-0236 et 13-01-0198) et a admis plusieurs cas. Il a toutefois maintenu ne pas être impliqué dans celui concernant Q. (MPC 13-01-0249). Lors de son audition du 10 novembre 2022, il a expliqué exclure ce cas en raison du pseudo « II. » qu'il a indiqué n'avoir jamais utilisé (MPC 13-01-0274).

Par-devant la Cour de céans, le prévenu a exposé contester le cas Q. parce qu'il aurait déjà arrêté de « travailler » lorsque celui-ci avait été réalisé (SK 37.731.027).

La Cour considère en droit :

1. Compétence de la Cour des affaires pénales du Tribunal pénal fédéral

1.1 La Cour examine d'office si sa compétence à raison de la matière est donnée au regard de l'art. 35 al. 1 de la loi fédérale sur l'organisation des autorités pénales de la Confédération (LOAP ; RS 173.71). Selon l'art. 24 al. 2 CPP, le MPC peut en particulier ouvrir une instruction pour des crimes visés au titre 2 du CP – soit les infractions contre le patrimoine, dont font partie les chefs de soustraction de données (art. 143 CP), accès indu à un système informatique (art. 143bis CP) et utilisation frauduleuse d'un ordinateur (art. 147 CP) – pour autant que le crime ait été commis pour une part prépondérante à l'étranger ou que dans plusieurs cantons sans qu'il y ait prédominance évidente dans l'un d'entre eux (let. a, en lien avec l'art. 24 al. 1 let. a et b CPP) et qu'aucune autorité cantonale de poursuite pénale ne soit saisie de l'affaire, respectivement que cette autorité ait sollicité la reprise de la procédure par le MPC (let. b). L'ouverture d'une instruction, par le MPC, en vertu de la disposition de l'art. 24 al. 2 CPP fonde la compétence fédérale (art. 24 al. 3 CPP).

1.2 En l'espèce, le MPC a accepté de reprendre la présente procédure du Ministère public neuchâtelois, par décision du 12 juin 2017, se fondant sur sa compétence dite facultative au sens de l'art. 24 al. 2 CPP, la cause présentant une ampleur exceptionnelle avec d'importants aspects d'extranéité (MPC 02-01-0006). La compétence de la Cour de céans est dès lors acquise (art. 24 al. 3 CPP).

2. Compétence territoriale suisse

2.1 Le code pénal suisse est applicable à quiconque commet un crime ou un délit en Suisse (art. 3 al. 1 CP). Aux termes de l'art. 8 al. 1 CP, un crime ou un délit est réputé commis tant au lieu où l'auteur a agi ou aurait dû agir qu'au lieu où le résultat s'est produit. Le lieu où l'auteur a agi ou aurait dû agir est le lieu où il a réalisé l'un des éléments constitutifs de l'infraction. Il suffit qu'il réalise partie – voire un seul – des actes constitutifs sur le territoire suisse (ATF 141 IV 336 consid. 1.1).

2.2 En l'espèce, il est constant que le prévenu et ses acolytes auraient agi depuis l'étranger, plus précisément Israël. Toutefois leurs démarches visaient exclusivement des sociétés suisses (SK 37.731.011), à savoir l'obtention de leurs données d'accès *e-banking* par connexion à distance sur un ordinateur de la société, en Suisse, et le détournement de leurs avoirs auprès de banques helvétiques. Le lieu de l'intrusion dans le système informatique se situe donc en Suisse, tout comme celui de la manipulation des données de la banque et le dommage patrimonial causé à la société par le débit de son compte. Partant, la compétence territoriale suisse est donnée, tant sous l'angle des chefs d'accusation de soustraction de données au sens de l'art. 143 CP et d'accès indu à un système informatique selon l'art. 143bis CP (décision de la Cour des plaintes BG.2012.37 du 24 janvier 2013, consid. 2.1 et références citées) que sous celui du chef d'utilisation frauduleuse d'un ordinateur au sens de l'art. 147 CP.

3. Appréciation des preuves et établissement des faits

3.1 Le Tribunal apprécie librement les preuves recueillies selon l'intime conviction qu'il se forge sur l'ensemble de la procédure (art. 10 al. 2 CPP). Garantie par l'art. 10 CPP, la présomption d'innocence a pour corollaire le principe *in dubio pro reo* qui concerne tant le fardeau de la preuve que l'appréciation des preuves. En tant que règle sur le fardeau de la preuve, ce principe signifie que celui-ci incombe à l'accusation et que le doute doit profiter à l'accusé. Il incombe entièrement et exclusivement à l'accusation d'établir la culpabilité du prévenu et non à celui-ci de démontrer qu'il n'est pas coupable. La présomption d'innocence est violée lorsque le juge rend un verdict de culpabilité au seul motif que l'accusé n'a pas prouvé son innocence. Comme règle d'appréciation des preuves, la

présomption d'innocence signifie que le juge ne doit pas se déclarer convaincu de l'existence d'un fait défavorable à l'accusé si, d'un point de vue objectif, il existe des doutes quant à l'existence de ce fait. Il importe peu qu'il subsiste des doutes seulement abstraits et théoriques, qui sont toujours possibles, une certitude absolue ne pouvant être exigée. Il doit s'agir de doutes sérieux et irréductibles, c'est-à-dire de doutes qui s'imposent à l'esprit en fonction de la situation objective. Ainsi, la présomption d'innocence se confond avec l'interdiction générale de l'arbitraire, prohibant une appréciation reposant sur des preuves inadéquates ou sans pertinence (ATF 127 I 38 consid. 2a ; arrêt du Tribunal fédéral 6B_1/2013 du 4 juillet 2013, consid. 1.5). L'examen de la suffisance des preuves obéit à des critères objectifs, alors que la conviction du juge se base sur l'impression d'ensemble qu'il se fait, en fonction du déroulement de la procédure, de la personnalité des parties et de la culpabilité du prévenu (PIQUEREZ/MACALUSO, Traité de procédure pénale suisse, 3e éd., 2011, n°579, p. 199).

3.2 En cas d'aveux, le ministère public et le tribunal s'assurent de la crédibilité de ses déclarations et l'invitent à décrire précisément les circonstances de l'infraction (art. 160 CPP). Un aveu peut être complet ou partiel, selon que le prévenu admette tout ou partie des faits qui lui sont reprochés tels que décrits par les autorités de poursuite pénale et doit être vérifié, et dans toute la mesure du possible circonstancié. La vérification des aveux a pour but de se prémunir contre les erreurs judiciaires qui trouvent le plus fréquemment leur source dans les faux aveux, qui eux-mêmes peuvent avoir les causes les plus diverses : affections psychiatriques, apathie, peur de la sanction, coercition physique ou psychologique lors des auditions, erreur sur les faits, protection de tiers, volonté d'aller en prison, recherche d'un alibi pour des actes plus graves ou infamants que ceux reprochés, etc. A noter que la toujours possible rétraction des aveux par le prévenu, résultant de son droit de s'exprimer librement et le cas échéant de s'autofavoriser, est une raison supplémentaire de procéder à la vérification des aveux et de conforter si possible ceux-ci par l'apport d'autres moyens de preuve. Par ailleurs, l'art. 160 CPP ne procède que partiellement de la libre appréciation des preuves, étant donné que, si celle-ci permet de prendre en compte la preuve par indices, et donc de prononcer une condamnation pénale sans qu'il y ait eu d'aveux, elle permet tout aussi bien de ne prendre en compte les aveux du prévenu que si ceux-ci sont crédibles. Cette précision s'évalue en fonction de la précision et de la cohérence des déclarations du prévenu qui reconnaît tout ou partie des faits (jugement de la Cour des affaires pénales SK.2017.7 du 29 mars 2018, consid. 2.7 et références citées).

3.3 Des cas admis par A. et de la fiabilité de ses aveux

3.3.1 En l'espèce, le prévenu a admis les faits qui lui sont reprochés au titre des cas G., anciennement G.a. (ch. 1.3.1 de l'acte d'accusation), I. (ch. 1.3.3 de l'acte d'accusation), H. (ch. 1.3.4 de l'acte d'accusation), K. (ch. 1.3.5 de l'acte d'accusation), B. (ch. 1.3.6 de l'acte d'accusation), R. (ch. 1.3.7 de l'acte d'accusation), N., anciennement N.a. (ch. 1.3.8 de l'acte d'accusation), C. (ch. 1.3.9 de l'acte d'accusation), L. (ch. 1.3.10 de l'acte d'accusation), D. (ch. 1.3.11 de l'acte d'accusation), E. (ch. 1.3.12 de l'acte d'accusation), O. (ch. 1.3.13 de l'acte d'accusation), M. (ch. 1.3.14 de l'acte d'accusation), P. (ch. 1.3.15 de l'acte d'accusation), la société 4 (ch. 1.3.16 de l'acte d'accusation), la société 5 (chiffre 1.3.17 de l'acte d'accusation), la société 6 (chiffre 1.3.18 de l'acte d'accusation), la société 38, aujourd'hui société 38.a. (chiffre 1.3.19 de l'acte d'accusation), la société 7 (chiffre 1.3.20 de l'acte d'accusation), la société 8 (chiffre 1.3.21 de l'acte d'accusation) et la société 39 (chiffre 1.3.22 de l'acte d'accusation).

3.3.2 Quant à ses motivations pour avouer ces faits, A. a indiqué être mu par sa volonté de tourner la page et ses remords (MPC 13-01-0242). Il a intégralement confirmé ses aveux par-devant la Cour de céans, alors qu'il était au bénéfice de mesures de substitution et avait été libéré de détention provisoire plus de deux ans auparavant (SK 37.731.014). Ses aveux sont riches en détails, notamment quant à des éléments factuels périphériques comme sa rencontre avec « EE. » ou la phase d'entraînement avec « FF. ». Aucun élément du dossier ne laisse penser que le prévenu pourrait avoir inventé son implication dans les fraudes ou fait l'objet de pressions pour avouer, à tort, les faits qui lui sont reprochés. Au contraire, A. a affirmé n'avoir pas collaboré plus tôt à l'enquête parce qu'il craignait des représailles (SK 37.731.017). Ainsi, s'il a ressenti des pressions, celles-ci l'ont poussé à nier les faits, et non les avouer.

3.3.3 Les aveux du prévenu sont corroborés par de nombreux autres moyens de preuve (cf. ch. E ss *supra*). En particulier, la réalité et le montant des détournements de fonds sont établis par pièces bancaires. Les agissements de A. sont par ailleurs démontrés par de multiples résultats d'enquête, en particulier des témoignages, des enregistrements audios et des analyses forensiques.

3.3.4 Ainsi, la Cour de céans constate que les aveux de A. sont non seulement parfaitement crédibles mais concordent aussi avec de nombreux autres moyens de preuve. Elle ne décèle aucun motif de mettre en doute leur véracité. Partant, elle tient pour établi les faits tels que reprochés à A. aux chiffres suivants de l'acte d'accusation : chiffres 1.3.1 (G., anciennement G.a.), 1.3.3 (I.), 1.3.4 (H.), 1.3.5 (K.), 1.3.6 (B.), 1.3.7 (R.), 1.3.8 (N., anciennement N.a.), 1.3.8 (C.), 1.3.10 (L.), 1.3.11 (D.), 1.3.12 (E.), ch. 1.3.13 (O.), 1.3.14 (M.), 1.3.15 (P.), 1.3.16 (société

4), 1.3.17 (société 5), 1.3.18 (société 6), 1.3.19 (société 38, aujourd'hui société 38.a.), 1.3.20 (société 7), 1.3.21 (société 8) et 1.3.22 (société 39).

3.4 Du cas F. (ch. 1.3.2 de l'acte d'accusation)

3.4.1 A. conteste toute implication dans ce cas, au motif qu'il serait antérieur au cas G.a. (aujourd'hui G.) et qu'il n'aurait pas perçu de « commission » correspondant aux montants détournés (cf. ch. F.2.4 *supra*).

3.4.2 En premier lieu, la Cour constate que le *modus operandi* des auteurs correspond manifestement à celui dont ont usé ensemble le prévenu, « GG. », « EE. » et « FF. » (cf. ch. F.2.3 et D *supra*) et que les raccordements utilisés l'ont également été dans d'autres cas perpétrés par ceux-ci et pour lesquels le prévenu a admis son implication (cf. ch. F.2.3 *supra*). Du reste, A. convient lui-même du fait que le cas est attribuable au même groupe d'auteurs, il a d'ailleurs affirmé que cette fraude était sûrement l'œuvre de « EE. » et « FF. » (cf. ch. F.2.4 *supra*) qui, selon le prévenu, ne se seraient dès lors pas adjoint son soutien ni celui de « GG. » pour ce cas-là.

3.4.3 En deuxième lieu, la Cour relève que le cas F. a été exécuté parallèlement à celui de G.a. (aujourd'hui G.), pour lequel le prévenu a admis son implication.

En effet, dans le cas F., une première prise de contact a eu lieu entre le 19 et le 22 décembre 2016. « HH.a. » a ensuite rappelé la société, le 22 décembre 2016, pour proposer à MM. de débuter la migration. Une troisième prise de contact a eu lieu le 22 décembre 2016, à 16h45, puis un premier transfert de fonds. Quelques jours plus tard, les 28 et 29 décembre 2016, « HH.a. » a à nouveau contacté la société, permettant le deuxième virement en cause (cf. ch. F.1 et F.2.3 *supra*).

Dans le cas G.a. (aujourd'hui G.), le prévenu a procédé à la première phase de la collecte d'informations. Il a, par la suite, le 22 décembre 2016 au matin, débuté la deuxième phase d'obtention des accès *e-banking* et a eu plusieurs autres contacts téléphoniques avec la société, jusqu'au début janvier 2017 (cf. ch. D.2.4 et F.2.4 *supra*).

L'enquête a du reste permis d'établir que les fraudes étaient perpétrées de manière parallèle et que les différentes phases de celle-ci pouvaient se recouper entre les cas (cf. ch. F.2.4 *supra*).

Ainsi, les auteurs n'ont pas exécuté les cas F. et G.a. (aujourd'hui G.) de manière séquentielle mais parallèle, comme cela ressort de la chronologie des appels des cas d'espèce, correspondant de surcroît au *modus operandi* habituel.

Au moment de l'exécution des cas F. et G.a. (aujourd'hui G.), le prévenu s'était déjà associé aux agissements criminels de « EE. » et s'entraînait depuis plusieurs jours avec « FF. » (cf. ch. D *supra).* A. a d'ailleurs admis le cas G.a. (aujourd'hui G.). Ainsi, la Cour constate que A. avait déjà débuté son activité criminelle aux côtés de ses acolytes lors de l'exécution du cas F.

3.4.4 En troisième lieu, la Cour retient que A., a, parfois, utilisé le pseudonyme « HH.a. », comme il l'a lui-même admis (cf. ch. D.2.3 *supra*).

Certes, le prévenu s'est rétracté par la suite (id). Il n'en demeure pas moins que ses premières déclarations – plus spontanées – paraissent particulièrement crédibles. Ceci d'autant plus que l'on ne perçoit pas comment le prévenu aurait pu se tromper et indiquer, par inadvertance, qu'il avait utilisé le pseudonyme « HH.a. ». Du reste, lors de ses premières déclarations, il a encore fourni des précisions quant à la fréquence avec laquelle il avait utilisé ce pseudonyme, en soulignant qu'il ne l'avait que peu employé (id).

De surcroît, les déclarations ultérieures du prévenu quant à ses pseudonymes ne sont pas exemptes de contradictions et donc peu crédibles. Ainsi, A. s'est non seulement rétracté s'agissant de son usage du pseudonyme « HH. », il a aussi nié avoir utilisé celui de « DD. », alors qu'il l'avait à plusieurs reprises confirmé auparavant (cf. ch. D.2.3 *supra*) et qu'il a, paradoxalement, confirmé aux débats avoir bien participé à une fraude, lors de laquelle il avait précisément utilisé le pseudonyme « DD. » (SK 37.731.029 et MPC 13-01-0266).

Enfin, il sied de relever que les pseudonymes « BB.a. » et « HH.a. » sont liés par le prénom employé. Les auteurs les ont parfois confondus dans leur utilisation, en particulier lorsque « FF. » a, par erreur, signé « HH.a. » un courriel, adressé à K., censé provenir de « BB.a. », pseudonyme utilisé par le prévenu pour contacter ladite société (cf. ch. F.2.3 *supra*). Cette proximité entre les deux pseudonymes et le fait que « FF. » les ait confondus renforce la conviction de la Cour que c'est bien A. qui, conformément à ses premières déclarations, utilisait (parfois) le pseudonyme « HH. ».

Ainsi, la Cour estime que les premières déclarations du prévenu quant à son usage du pseudonyme « HH. » sont singulièrement plus crédibles que ses dénégations ultérieures. L'utilisation, par A., dudit pseudonyme est d'ailleurs corroborée par le fait que son acolyte « FF. » s'y soit référé (par erreur) pour les besoins d'une fraude perpétrée par le prévenu, à qui « FF. » associait le pseudonyme « HH. ». La Cour tient ainsi pour établi que le prévenu a bien, parfois, utilisé ce pseudonyme.

3.4.5 En quatrième lieu, la Cour constate qu'il est complètement invraisemblable que « EE. » ou « FF. » – ou un autre comparse – aient utilisé le pseudonyme « HH.a. », pour contacter F., et non le prévenu, comme il l'a suggéré (cf. ch. F.2.4 *supra)*. En effet, selon A., « FF. » et « EE. » accordaient beaucoup d'importance à ce que le prévenu et « GG. » utilisent toujours leurs différents pseudonymes respectifs dans leurs contacts avec les lésés (cf. ch. D.2.4 *supra*). Il eut donc été contradictoire pour « FF. » ou « EE. » d'utiliser eux-mêmes un des pseudonymes du prévenu, ceci de surcroît alors que A. avait déjà débuté son activité criminelle (cf. ch. 3.4.3 *supra*). Ce dernier a d'ailleurs lui-même exclu que « FF. » et « EE. » aient utilisé le pseudonyme « HH. » (cf. ch. F.2.4 *supra*).

3.4.6 En cinquième lieu, la Cour relève que les deux raccordements utilisés pour le cas F. ont également été utilisés, à la même période (fin décembre 2016 à début janvier 2017), pour les autres cas commis au cours de celle-ci et qui ont été reconnus par le prévenu, soit les cas G.a., aujourd'hui G., I., K. et H. (cf. ch. F.2.3 *supra*). En particulier, le 22 décembre 2016, à 10h23, l'auteur de l'appel à F. a indiqué qu'on pouvait le rappeler au 15, soit un des deux raccordements utilisés par le prévenu pour appeler G.a., aujourd'hui G., à cinq reprises, entre le 22 et le 23 décembre 2016. Or, à teneur des explications du prévenu, les deux téléphones portables utilisés pour contacter les sociétés lésées restaient posés sur son bureau pour l'éventualité où l'employé de la société rappellerait, afin que les personnes présentes – soit « GG. », « FF. » et le prévenu – puissent décrocher et leur répondre. Ces derniers utilisaient le même raccordement pendant quelques jours et pour quelques cas, avant d'en changer (id.). Partant, il est totalement invraisemblable qu'un tiers – autre que le prévenu et ses acolytes – ait indiqué à F. de le rappeler, fin décembre 2016, sur des numéros se trouvant alors en leur possession et qu'ils étaient précisément en train d'utiliser pour effectuer des fraudes, notamment pour recevoir des appels des sociétés lésées. Or, selon les déclarations du prévenu, ni « FF. » ni « EE. » n'utilisaient le pseudonyme « HH. » ; seul lui l'avait, parfois, utilisé (cf. ch. 3.4.4 s. *supra*).

3.4.7 En sixième lieu, la Cour constate que même si A. devait n'avoir pas perçu de « commission » correspondant au montant des fonds détournés de F., cela ne permettrait pas d'en déduire qu'il n'a pas participé au cas.

En effet, A. a déclaré avoir été « volé » par « FF. » et « EE. », qui ne lui avaient pas toujours remis le montant des « commissions » qui lui revenaient et à « GG. » (cf. ch. D.2.6 *supra*). L'ampleur de ces « vols » subis par le prévenu aurait été important, dès lors qu'il affirme avoir perçu, au total, au maximum EUR 200'000.- soit moins de la moitié de la part du butin lui revenant selon la clé de répartition convenue, évaluée à EUR 454'468.41 (0.09 x EUR 5'049'649.-; cf. ch. D.1.4 et D.2.6 *supra* ; SK 37.731.021). Même sans tenir compte de la part du prévenu au butin provenant du cas F., soit EUR 171'459.- (0.09 x EUR 1'905'102.- ; cf. ch. F.2.1 *supra*), A. aurait été « volé » de près d'un tiers de

ses « commissions » sur les autres cas également. Ainsi, les « commissions » effectivement perçues par le prévenu – selon ses dires – sont sans commun rapport avec l'ampleur de ses expectatives y relatives, telles qu'elles découlaient de la clé de répartition du butin convenue, et de la réelle ampleur de son activité délictuelle. Partant, le montant total des « commissions » effectivement perçues, selon les dires du prévenu, ne permet pas de déduction quant à son implication dans le cas d'espèce spécifique.

Du reste, la Cour constate que A. s'est montré réticent à admettre son implication et prendre ses responsabilités lorsqu'il n'avait (selon ses dires) pas perçu la « commission » lui revenant, soit lorsqu'il n'aurait pas été rétribué selon ses expectatives pour ses méfaits, ceci y compris après avoir pourtant déclaré au MPC qu'il voulait désormais s'expliquer. Ainsi, il a encore – par deux fois – maintenu ses dénégations s'agissant du cas C., parce qu'il n'avait pas perçu sa « commission » (cf. ch. F.2.4 *supra*), ceci bien qu'il savait pertinemment avoir participé au cas, se souvenant même s'être disputé avec « EE. » dans ce contexte, comme il l'a finalement admis par la suite (id.). Il sied de relever qu'il eut été particulièrement malaisé pour le prévenu de maintenir ses dénégations concernant le cas C., dès lors qu'il avait utilisé son pseudonyme habituel de « BB. » pour le perpétrer.

3.4.8 En septième lieu, la Cour constate que le prévenu a minimisé la durée de ses agissements criminels, ceci également après avoir annoncé au MPC qu'il voulait désormais s'expliquer. Il a ainsi d'abord indiqué avoir (provisoirement) cessé les fraudes après son engagement par la société 11, avant d'admettre avoir, en fait, alors poursuivi ses agissements pendant deux mois (cf.ch. D.2.8 *supra*). Partant, les indications du prévenu quant à la durée de ses agissements paraissent sujettes à caution, y compris s'agissant de ses appels au mois de décembre 2016.

3.4.9 Au vu de ces éléments, la Cour est convaincue que A. a parfois utilisé le pseudonyme « HH. », conformément à ses premières déclarations, et qu'il a contacté F. sous ce nom, selon le *modus operandi* habituel et avec les raccordements qu'il utilisait alors pour commettre les fraudes, ayant déjà débuté son activité criminelle. Il n'existe pas de doute sérieux et irréductible quant au déroulement des faits, tels que décrits sous chiffre 1.3.2 de l'acte d'accusation, y compris sous l'angle de l'identité de l'auteur agissant sous le pseudonyme « HH. » – soit A. – que la Cour tient pour établis.

3.4.10 Enfin, par surabondance et sans que cet élément soit retenu comme un indice à charge du prévenu – la présente précision s'avérant toutefois nécessaire sous l'angle du droit d'être entendu du prévenu, dès lors que la défense a plaidé, comme indice à décharge, que A. n'aurait pas d'intérêt à nier son implication dans le cas F., au vu de la proportion élevée de cas admis (SK 37.721.067 s.) –

, il sied encore de relever que le prévenu a bien un intérêt à contester toute implication dans le cas F., les détournements de fonds à son détriment portant sur la somme totale de CHF 2'053'007.93 (monnaie du compte) resp. EUR 1'905'102.- (monnaie de la transaction ; cf. ch. F.1.6 *supra*), soit plus d'un tiers du montant des détournements cumulés reprochés au prévenu. La défense s'est d'ailleurs prévalue de l'impact sur la peine d'un acquittement pour le cas F. (SK 37.721.092). Ainsi, le prévenu voit bien un intérêt pratique à contester son implication dans le cas en question, bien qu'il ait, par ailleurs, admis la grande majorité des cas qui lui sont reprochés.

3.5 Du cas J. (chiffre 1.3.23 de l'acte d'accusation)

3.5.1 Le prévenu conteste son implication dans le cas J. au motif que, selon lui, celui-ci serait antérieur au cas concernant G.a., aujourd'hui G. (cf. ch. AA.2 *supra*).

3.5.2 En premier lieu, la Cour constate que le *modus operandi* des auteurs correspond à celui dont ont usé le prévenu, « GG. », « EE. » et « FF. » et que le raccordement employé par « BB. » pour contacter la société J. (17) est celui que le prévenu a utilisé pour contacter, entre le 22 décembre 2016 et 16 janvier 2017, les sociétés G.a. (aujourd'hui G.), H., I., K. et B. (cf. ch. AA.2.1 *supra*).

Manifestement, l'appel à J. émane du même cercle d'auteurs.

3.5.3 En deuxième lieu, la Cour relève que le pseudonyme utilisé par l'auteur de l'appel est « BB. », soit un de ceux que A. avait l'habitude d'utiliser (cf. ch. AA.1 ss et D *supra*).

Il apparaît complètement invraisemblable que « EE. » ou « FF. » – ou un autre comparse – aient utilisé le pseudonyme « BB. », pour contacter la société J., et non le prévenu, de surcroît à une date (21 décembre 2016) où le prévenu s'était déjà associé aux agissements criminels de « EE. » et s'entraînait depuis plusieurs jours avec « FF. » (cf. ch. AA.1 ss et D *supra)*. En effet, comme l'a expliqué le prévenu, « FF. » et « EE. » accordaient beaucoup d'importance à ce que le prévenu et « GG. » utilisent toujours leurs différents pseudonymes respectifs dans leurs contacts avec les lésés (cf. ch. D.2.4 *supra*). Il eut donc été contradictoire pour eux d'utiliser eux-mêmes un des pseudonymes du prévenu ou qu'une autre personne pratiquant des fraudes selon exactement le même *modus operandi* ait, elle aussi, utilisé le pseudonyme « BB. », comme le faisait le prévenu, ceci, de surcroît, alors que ce dernier avait déjà débuté son activité criminelle. De plus, selon le prévenu, seuls « GG. », « FF. » et « EE. » travaillaient avec lui (id).

3.5.4 En troisième lieu, la Cour constate qu'il est parfaitement vraisemblable que A. ait effectué son premier appel à G.a., aujourd'hui G., avant le 22 décembre 2016 et qu'il ait perpétré les deux cas en parallèle. Dans le cas G.a., aujourd'hui G., c'est la deuxième phase d'acquisition des identifiants *e-banking* qui a débuté le 22 décembre 2016. Or, A. a indiqué avoir aussi procédé à la (première) phase de collecte d'informations, antérieurement (cf. ch. AA.2.2 *supra*). La prise de contact avec J. date, elle, du 21 décembre 2016. Il n'est donc pas possible de constater que les deux cas auraient été exécutés de manière séquentielle et que l'un aurait été perpétré antérieurement à l'autre.

3.5.5 En quatrième lieu, la Cour rappelle que le prévenu a minimisé la durée de ses agissements criminels, ceci également après avoir annoncé au Procureur qu'il voulait désormais s'expliquer. Il a ainsi d'abord indiqué avoir (provisoirement) cessé les fraudes après son engagement par la société 11, avant d'admettre avoir alors poursuivi ses agissements pendant deux mois (cf.ch. D.2.8 *supra*). Partant, les indications du prévenu quant à la durée de ses agissements paraissent sujettes à caution, y compris s'agissant de ses appels au mois de décembre 2016.

3.5.6 Compte tenu de ce qui précède, il n'existe aucun doute sérieux quant au fait que A., agissant sous le pseudonyme de « BB. », a contacté la société J. le 21 décembre 2016, selon les faits décrits au chiffre 1.3.23 de l'acte d'accusation. La Cour tient dès lors ces faits pour établis.

3.5.7 Dans la mesure où la défense s'est prévalue, à décharge, que A. n'aurait aucun intérêt à nier son implication dans le cas J., alors qu'il en a admis beaucoup d'autres (SK 37.721.067 s.), il s'impose à la Cour de relever ce qui suit, conformément au droit d'être entendu du prévenu, mais toutefois sans que ce constat soit retenu à charge de celui-ci : il eut été malaisé pour le prévenu de reconnaître son implication dans le cas J. – le 21 décembre 2016 – tout en maintenant ses dénégations pour celui de F. Or, le prévenu a un intérêt tangible à contester toute implication dans ce deuxième cas, les détournements de fonds à son détriment portant sur plus d'un tiers du montant des détournements cumulés qui lui sont reprochés. La défense s'est d'ailleurs prévalue de l'impact sur la peine d'un acquittement pour le cas F. (SK 37.721.092). Ainsi, le prévenu voit bien un intérêt pratique à contester son implication dans le cas en question, bien qu'il ait, par ailleurs, admis la grande majorité des autres cas qui lui sont reprochés (cf. ch. 3.4.10 *supra*).

3.6 Du cas de la société 9 (chiffre 1.3.24 de l'acte d'accusation)

3.6.1 La Cour constate que le pseudonyme utilisé dans le cas de la société 9, « JJ. » ne fait pas partie de ceux que le prévenu a admis avoir utilisés. Contrairement aux pseudonymes « BB. », « CC. », « HH. » et « DD. », le prévenu a contesté de manière constante l'utilisation de « JJ. », respectivement « KK. » (cf. ch. D.2.4 et BB.2.4 *supra).* L'enquête n'a pas non plus permis d'établir autrement un lien personnel entre le prévenu et ce pseudonyme, y compris dans le contexte des investigations quant au cas de la société 3, classé faute de preuve (cf. ch. A.13 *supra*).

3.6.2 Dès lors, bien que tant le *modus operandi*, que le raccordement utilisé convergent et qu'il puisse en être déduit que l'appel à la société 9 relève du même type de fraude que celles commises par le prévenu et ses acolytes (cf. ch. BB.2.1 ss *supra*), la Cour estime qu'il subsiste néanmoins des doutes quant à l'implication personnelle de A. dans celle-ci, dès lors qu'il conteste l'utilisation du pseudonyme « JJ. » et que son utilisation n'a pu être prouvée d'une autre manière. Au vu des résultats d'enquête, il apparaît possible qu'un des acolytes du prévenu ait utilisé le pseudonyme « JJ. » et soit l'auteur de l'appel en cause, ce d'autant plus que l'appelant « KK. » (respectivement « JJ. ») dans le cas de la société 3 avait appelé la société depuis un raccordement différent de celui utilisé par « BB. » (cf. ch. BB.2.2 *supra*).

3.6.3 Le doute de la Cour devant profiter à A., elle doit constater qu'il n'est pas établi que le prévenu soit le dénommé « JJ. » ayant contacté la société 9 et, ainsi, acquitter le prévenu de tout chef de prévention en lien avec ledit cas, selon le chiffre 1.3.24 de l'acte d'accusation.

3.7 Du cas Q. (chiffre 1.3.25 de l'acte d'accusation)

3.7.1 La Cour constate que le pseudonyme utilisé dans le cas Q., « II.a. » ne fait pas non plus partie de ceux que le prévenu a admis avoir utilisés. Contrairement aux pseudonymes « BB. », « CC. », « HH. » et « DD. », le prévenu a contesté de manière constante l'utilisation du pseudonyme « II.a. » (cf. ch. D.2.3 et CC.2.3 *supra).* L'enquête n'a pas non plus permis d'établir autrement un lien personnel entre le prévenu et ce pseudonyme. En effet, il semble que l'adresse au nom de « HH.a. » ait été utilisée à d'autres fins que celles de l'obtention des accès *e-banking*, soit en particulier pendant la première phase de la collecte d'informations en amont, et ce dans de nombreux cas dont seul celui de Q. est reproché au prévenu (cf. ch. CC.2.3 *supra*). Dans le contexte de l'appel de « II.a. », c'est encore une autre adresse e-mail, au nom de ce dernier (II.a.@cyberservices.com), qui a été utilisée.

3.7.2 Dès lors, bien que le *modus operandi* et l'utilisation d'une adresse mail au nom de « HH.a. » apparaissent comme des indices convergents laissant présupposer que Q. a bien été visé par le même type de fraude que celles commises par le prévenu et ses acolytes (cf. ch. CC.2.1 ss *supra*) et tout en considérant peu crédibles les dénégations du prévenu aux débats, selon lesquelles il n'aurait plus été actif dans les fraudes alors qu'il avait précédemment confirmé avoir repris ces activités pendant les mois de mai à août 2018 (cf. ch. CC.2.3 *supra*), la Cour estime qu'il subsiste néanmoins des doutes quant à l'implication personnelle de A. dans celle-ci. En effet, il conteste l'utilisation du pseudonyme « II.a. » et son utilisation n'a pu être prouvée d'une autre manière. Au vu des résultats d'enquête, il apparaît possible qu'un des acolytes du prévenu ait utilisé le pseudonyme « II.a. » et soit l'auteur de l'appel en cause.

3.7.3 Le doute de la Cour devant profiter à A., elle doit constater qu'il n'est pas établi que le prévenu soit le dénommé « II.a. » qui a contacté la société Q. et, ainsi, acquitter le prévenu de tout chef de prévention en lien avec ledit cas, selon chiffre 1.3.25 de l'acte d'accusation.

3.8 Des cas imputables à A. et du préjudice causé

3.8.1 Comme détaillé ci-avant, la Cour tient pour établi les faits tels que décrits aux chiffres 1.3.1 à 1.3.23 de l'acte d'accusation.

3.8.2 L'implication de A. dans des fraudes ayant concerné 23 sociétés différentes est donc avérée. Ces fraudes ont été commises au cours de la période allant de décembre 2016 à décembre 2017, puis entre mai et juillet 2018. Dans ce contexte, les auteurs ont passé des ordres de débit pour un montant d'une contre-valeur totale d'environ CHF 9 millions, depuis les comptes des sociétés lésées. Sur l'ensemble des ordres passés, des transferts correspondant à un montant total d'environ CHF 5 millions (EUR 4'374'742.- + CHF 722'151.- [correspondant à EUR 674'907.- au 24 janvier 2017, date de la transaction], soit EUR 5'049'649.-) ont été exécutés et n'ont pas pu être recouverts (cf. ch. D.1.4 *supra*). Ces fonds ont ainsi effectivement pu être détournés par les auteurs (butin). Le solde des transferts ordonnés par ceux-ci, soit environ CHF 4 millions au total (EUR 3'149'148.70 + CHF 720'000.-), n'a soit pas été exécuté par la banque de la société – il s'agit des tentatives proprement dites – ou les fonds ont pu faire l'objet d'un blocage (par la banque de destination) et d'un rapatriement ultérieur (cf. ch. E.1.7, H.1.4, K.2.1, M.2.2, O.1.4, P.2.4, Q.1.2 et R.1.2 *supra*).

3.8.3 Il convient dès lors d'examiner la qualification juridique de ces faits, étant rappelé que la Cour a réservé leur appréciation à l'aune des art. 147 al. 1 et 2 CP (utilisation frauduleuse d'un ordinateur par métier), à l'exclusion des art. 143 CP (soustraction de données) et 143bis CP (accès indu à un système informatique).

4. Qualification juridique des faits

4.1 Du chef d'utilisation frauduleuse d'un ordinateur (art. 147 CP)

4.1.1 L'art. 147 aCP, en sa teneur jusqu'au 1er juillet 2023, réprime, par une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire, le comportement de celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime aura, en utilisant des données de manière incorrecte, incomplète ou indue ou en recourant à un procédé analogue, influé sur un processus électronique ou similaire de traitement ou de transmission de données et aura, par le biais du résultat inexact ainsi obtenu, provoqué un transfert d'actifs au préjudice d'autrui ou l'aura dissimulé aussitôt après (al. 1). Si l'auteur fait métier de tels actes, la peine sera une peine privative de liberté de dix ans au plus ou une peine pécuniaire de 90 jours-amende au moins (al. 2).

La peine menace applicable a été modifiée par la réforme du Code pénal entrée en vigueur le 1er juillet 2023 (harmonisation des peines). Ainsi, l'infraction, dans sa forme qualifiée, est aujourd'hui passible d'une peine privative de liberté de 6 mois à 10 ans, alors qu'elle était jusqu'alors réprimée, alternativement, par une peine privative de liberté de 10 ans au plus ou d'une peine pécuniaire de 90 jours-amende au moins. La peine menace actuelle étant plus lourde et, ainsi, pas plus favorable au prévenu, c'est celle en vigueur au moment des faits qui devrait en principe s'appliquer (art. 2 CP). La modification législative entrée en vigueur le 1er juillet 2023 apparaît cependant sans importance sous l'angle de la *lex mitior*, dans la mesure où la peine qui va être retenue pour cette infraction est supérieure à 6 mois (cf. ch. 7 *infra*).

4.1.2 L'infraction d'utilisation frauduleuse d'un ordinateur, qui est une infraction dirigée contre le patrimoine, suppose, sur le plan objectif (i) une manipulation de données sous la forme d'une utilisation de données de manière incorrecte, incomplète ou indue ou d'un procédé analogue, (ii) l'influence de cette manipulation sur un processus électronique ou similaire de traitement ou de transmission de données, (iii) de telle sorte qu'un résultat inexact soit obtenu et (iv) que la manipulation aboutisse à un transfert d'actifs (ou sa dissimulation) (v) causant un dommage patrimonial à autrui. Sur le plan subjectif, elle implique que l'auteur ait agi intentionnellement et dans un dessein d'enrichissement illégitime. Avec la clause générale " (...) à un procédé analogue (...) ", le législateur voulait faire en sorte que toutes les possibilités de manipulation à venir puissent également être visées (arrêt du Tribunal fédéral 6B_683/2021 du 30 mars 2022, consid. 5.1.1 et les réf. ; DUPUIS/MOREILLON/PIGUET/ BERGER/MAZOU/RODIGARI, Petit Commentaire du Code pénal, 2ème éd. 2017, n° 1 ad art. 147 CP).

4.1.3 L'infraction réprimée par l'art. 147 CP (ou aCP) s'apparente à l'escroquerie (art. 146 CP), dont elle se distingue toutefois en cela que l'auteur ne trompe pas un être humain pour le déterminer ainsi à des actes préjudiciables à ses intérêts pécuniaires ou à ceux d'un tiers, mais manipule une machine de manière à obtenir un résultat inexact aboutissant à un transfert d'actifs ou à sa dissimulation. En d'autres termes, au lieu de tromper une personne, l'auteur fausse les conditions qui déterminent la réaction de la machine (arrêt du Tribunal fédéral 6B_683/2021 du 30 mars 2022, consid. 5.1.1 et références citées). Le comportement analogue à une escroquerie réside dans le fait que l'auteur, par ses agissements, feint d'être autorisé à utiliser les données, alors que tel n'est pas le cas (arrêt du Tribunal fédéral 6B_549/2023 du 25 septembre 2023, consid. 2.3 et références citées). La manière avec laquelle il obtient ces données ne joue aucun rôle (id.). Par ailleurs, si l'art. 146 CP présuppose un acte de disposition du lésé, l'art. 147 CP exige, lui, un transfert de patrimoine effectué par l'ordinateur, au détriment de tiers, par exemple par le versement d'un montant en espèces, par un crédit sur un compte ou par l'omission d'un débit sur un compte. Comme dans le cas de l'escroquerie au sens de l'art. 146 CP, le transfert de patrimoine doit entraîner un préjudice financier (arrêt du Tribunal fédéral 6B_831/2023 du 24 avril 2024, consid. 4.8.2).

4.1.4 Il y a manipulation de données par une utilisation indue de celles-ci lorsque l'auteur utilise des données correctes mais qu'il n'est pas autorisé à le faire, par exemple lorsqu'il utilise une carte bancaire volée, le code d'autrui, obtient des données par le système d'hameçonnage ou encore emploie sans droit le système informatique d'un tiers (DUPUIS ET AL., *op. cit.*, n° 12 ad art. 147 CP et références citées ; GRODECKI, in Commentaire romand du Code pénal II, 2ème éd. 2025 [ci-après : CR-CP], n° 9 ad art. 147 CP).

4.1.5 La manipulation doit encore influencer le processus de traitement ou de transmission des données en ce que le résultat obtenu ne correspond pas à celui qui serait survenu si le processus s'était déroulé normalement (GRODECKI, in CR-CP, n° 11 ad art. 147 CP ; FIOLKA, in Commentaire bâlois du Code pénal, 4ème éd. 2019 [ci-après : BSK-StGB], n° 36 ad art. 147 CP).

4.1.6 La réalisation de l'infraction présuppose également un dommage patrimonial consistant en un transfert de fonds ou la naissance d'une dette (GRODECKI, in CR-CP, n° 15 ad art. 147 CP ; FIOLKA, in BSK-StGB, n° 437 s. ad art. 147 CP). Il y a un transfert d'actif en cas de passage d'argent d'un compte à un autre ou lorsqu'il y a naissance d'une dette (GRODECKI, in CR-CP, n° 13 ad art. 147 CP).

4.1.7 Conformément à la jurisprudence, l'auteur agit par métier (au sens de l'art. 147 al. 2 CP) lorsqu'il résulte du temps et des moyens qu'il consacre à ses agissements délictueux, de la fréquence des actes pendant une période déterminée, ainsi que des revenus envisagés ou obtenus, qu'il exerce son activité

coupable à la manière d'une profession, même accessoire ; il faut que l'auteur aspire à obtenir des revenus relativement réguliers représentant un apport notable au financement de son genre de vie et qu'il se soit ainsi, d'une certaine façon, installé dans la délinquance (arrêt du Tribunal fédéral 6B_683/2021 du 30 mars 2022, consid. 5.1.2 et références citées). L'auteur doit avoir agi à plusieurs reprises, avoir eu l'intention d'obtenir un revenu et être prêts à réitérer ses agissements. Il n'est pas nécessaire que ceux-ci constituent sa principale activité professionnelle, une activité « accessoire » illicite peut aussi être exercée par métier. A noter que le fait que l'auteur utilise les sommes provenant de son activité délictueuse à des fins inutiles n'exclut pas la perpétration par métier (GRODECKI, in CR-CP, n° 21 ad art. 147 CP).

4.1.8 Il y a tentative lorsque l'auteur a réalisé tous les éléments subjectifs de l'infraction et manifesté sa décision de la commettre, alors que les éléments objectifs font, en tout ou en partie, défaut (parmi d'autres, arrêt du Tribunal fédéral 6B_231/2025 du 6 août 2025, consid. 2.1). La tentative est absorbée par le délit consommé par métier lorsque l'auteur a commis plusieurs tentatives et des délits consommés (ATF 123 IV 113 consid. 2d). Lorsque la qualification de métier s'applique, elle exclut un concours entre les différents actes, lesquels forment alors une seule entité juridique, qui comprend aussi bien les actes tentés que les actes consommés (jugement de la Cour des affaires pénales SK.2023.18 du 21 juin 2023, consid. 4.1.8 et références citées).

4.1.9 A teneur de l'art. 49 al. 1 CP, si en raison d'un ou de plusieurs actes, l'auteur remplit les conditions de plusieurs peines du même genre, le juge le condamne à la peine de l'infraction la plus grave et l'augmente dans une juste proportion. Il ne peut toutefois excéder de plus de la moitié le maximum de la peine prévue pour cette infraction. Il est en outre lié par le maximum légal de chaque genre de peine.

En concours avec l'art. 147 CP, la soustraction de données (art. 143 CP) est absorbée comme acte préparatoire (TPF 2021 83 consid. 3.4), à tout le moins en cas d'identité entre les lésés des deux infractions (SCHMID, Kommentar Computer sowie Check- und Kreditkartenkriminalität, Zürich 1994, p. 173, n° 38 s.) et que la soustraction de données et l'utilisation frauduleuse d'un ordinateur n'apparaissent pas comme des processus échelonnés ou que les données présentent une valeur patrimoniale propre pour l'auteur (FIOLKA, in BSK-StGB, n° 47 ad art. 147 CP).

A son tour, la soustraction de données de l'art. 143 CP absorbe entièrement l'accès indu réprimé par 143bis CP (WEISSENBERGER, in BSK-StGB, n° 41 ad art. 143 CP ; MONNIER, in CR-CP, n° 21 ad art. 143 CP).

4.2 Du cas d'espèce

4.2.1 Dans l'ensemble des 23 cas, A. a exécuté la deuxième phase de la fraude, en collaboration directe avec « FF. », à savoir celle consistant pour lui à contacter la société en se faisant passer pour un informaticien de la banque, amener son interlocuteur à se connecter à distance à l'ordinateur de « FF. » et, ainsi, obtenir les accès *e-banking* de la société. Cette démarche s'inscrivait dans le cadre d'un processus défini et rôdé visant *in fine* à utiliser les accès *e-banking* des sociétés démarchées pour détourner leurs avoirs bancaires par des débits frauduleux.

4.2.2 Le prévenu et ses acolytes ont ainsi utilisé les accès *e-banking* – obtenus grâce aux démarches de A. et la mise en place du contrôle à distance – c'est-à-dire des données correctes, introduites par l'employé de la société dans son ordinateur. Dans certains cas, le prévenu et « FF. » prenaient connaissance des accès en les visualisant à leur écran, lorsque l'employé de la société les introduisait sur son ordinateur, puis ces accès étaient utilisés depuis un autre appareil, en ouvrant une nouvelle session. Dans d'autres cas, ils utilisaient ces accès directement depuis l'ordinateur de l'employé et la session *e-banking* ouverte par ce dernier. Dans les deux cas de figure, le prévenu et ses acolytes n'étaient pas habilités à utiliser les accès *e-banking* de la société et d'ainsi accéder à ses comptes pour passer des ordres de paiement au débit de ceux-ci (utilisation indue). En utilisant ces accès pour passer des ordres bancaires, les auteurs ont feint d'être autorisés à effectuer ces opérations au nom de la société titulaire du compte (influence sur le processus électronique), manœuvre couronnée de succès et qui a abouti au résultat que les serveurs bancaires ont conclu, à tort, que les titulaires des comptes, respectivement des personnes disposant des droits de signature sur ceux-ci, voulaient effectuer, au nom de la société, les versements ordonnés et ont enregistré les ordres passés (obtention d'un résultat inexact). Ces derniers, lorsqu'ils ont été exécutés par la banque de la société, ont occasionné des transferts de fonds portés au débit du compte (transferts d'actifs), réduisant d'autant le patrimoine de la société (dommage patrimonial). A chaque prise de contact avec une société démarchée, A. (et ses acolytes) savaient qu'ils obtenaient les accès *e-banking* de celle-ci à son insu, qu'ils n'étaient pas habilités à les utiliser et qu'ils les employaient pour passer des ordres bancaires sans l'autorisation du titulaire du compte. Ils ont agi précisément dans le but de procéder à des versements depuis ces comptes et faire transiter les fonds ainsi soustraits aux sociétés par des mules financières. Ultimement, les fonds détournés leur reviendraient par une participation au butin, ce qu'ils savaient également et appelaient de leurs vœux (intention et dessein d'enrichissement illégitime).

4.2.3 A. a exercé son activité criminelle entre décembre 2016 et juillet 2018, soit durant 20 mois, et les 23 cas pour lesquels la Cour le condamne ont été commis sur six mois différents. Durant cette période, le prévenu a poursuivi cette activité à la manière d'un travail, dont il tirait un revenu fixe mensuel de EUR 6'000.-, son « salaire » et une « commission », gratification dépendant des sommes effectivement détournées de ses « clients ». Il a ainsi généré des revenus conséquents par son activité criminelle estimés, pour les 23 cas en cause, à six salaires mensuels de EUR 6'000.- et des « commissions », par EUR 454'468.41, soit au total EUR 490'468.41 (6 x EUR 6'000.- + EUR 454'468.41). La question de savoir si le prévenu a, comme il l'affirme, lui-même été « volé » par ses acolytes en ne touchant pas l'entier des « commissions » qui lui étaient dues concerne des faits ultérieurs aux agissements proprement dits pour lesquels il est condamné et n'est, à ce titre, pas pertinente pour déterminer l'ampleur de l'activité criminelle du prévenu, les revenus qu'il escomptait tirer de celle-ci au moment de la commission de l'infraction et la manière avec laquelle il la perpétrait. Par comparaison avec ses revenus mensuels avant qu'il ne débute les fraudes, soit ILS 25'000.- à ILS 30'000.- (entre CHF 6'250.- et CHF 7'500.- ; SK.37.731.004), A. a très considérablement amélioré ses finances par le crime, à raison d'au moins EUR 24'523.- par mois (EUR 490'468.41/20), ce dont il était parfaitement conscient et voulait, étant non seulement informé du volume des détournements mais aussi rémunéré quelques jours plus tard, et ayant néanmoins poursuivi ses activités criminelles. Il n'en irait pas autrement même si les revenus de provenance criminelle du prévenu n'avaient pas excédé un total de EUR 200'000.-, soit au moins EUR 10'000.- par mois (EUR 200'000.-/20). Enfin, on relèvera que ce n'est qu'après avoir trouvé une activité professionnelle licite que A. aurait, provisoirement, mis un terme à son engagement dans les fraudes début 2018, avant de reprendre celles-ci en mai de la même année (cf. ch. D.2.6 ss *supra*). Partant, il a non seulement agi à réitérées reprises, selon un *modus operandi* défini, mais a aussi, par ses agissements, cherché à améliorer sa situation financière par des revenus criminels, de surcroît réguliers. Le fait que A. aurait utilisé l'entier de ses revenus de source délictuelle pour des divertissements comme des voyages ou des habits, ou encore, dans une faible mesure, pour des œuvres de charité (cf. ch. D.2.6 *supra*) – soit très principalement pour des dépenses personnelles et non pour subvenir aux besoins de sa famille – n'exclut pas la perpétration par métier. Ainsi, la qualification du métier s'applique au cas d'espèce.

4.2.4 Les conditions objectives et subjectives du chef d'utilisation frauduleuse d'un ordinateur qualifié, telles qu'énoncées à l'art. 147 al. 1 et 2 CP, sont ainsi remplies pour l'ensemble des infractions consommées, soit chaque fois lorsque le compte d'une société a effectivement été débité.

Les conditions subjectives des mêmes dispositions sont également réalisées pour chaque opération tentée (sans débit des comptes des sociétés), soit lorsque la transaction n'a pas été exécutée par la banque et que A. et ses acolytes n'ont pas réussi à mener la fraude à son terme, malgré la prise de contact par le prévenu en vue de l'acquisition des accès *e-banking*, faute d'avoir réussi à établir le contrôle à distance, d'obtenir les accès *e-banking* nécessaires ou d'exécution de l'ordre par la banque.

Ainsi, les conditions des art. 147 al. 1 et 2 CP sont réunies pour l'ensemble des 23 cas dans lesquels A. est impliqué et pour tous lesquels il a effectué – au moins (cf. ch. D. 2.4 et D.2.5 *supra*) – la deuxième phase de la fraude, soit celle de l'acquisition des accès *e-banking*.

4.2.5 Dès lors que la qualification du métier s'applique *in casu*, les différents actes forment une unité juridique, comprenant aussi bien les actes tentés (sans débit des comptes des sociétés) que les actes consommés (exécution des ordres de débit).

Il y a également unité dans la décision du prévenu de passer à l'acte et commettre les 23 cas, y compris en ce qui concerne ceux perpétrés dès mai 2018, soit à l'issue d'une pause (provisoire) dans son activité criminelle au début de la même année. En effet, les motivations principales de A. sont restées les mêmes, soit l'appât du gain, et sa volonté délictuelle demeurait inchangée. Certes, aux débats, le prévenu a avancé que c'est la crainte que lui inspirait « EE. » qui l'aurait motivé à reprendre les fraudes, en mai 2018 (SK 37.731.020). En instruction, il avait toutefois expliqué n'avoir jamais subi de menaces ou de pression en liens avec les faits, bien qu'il ait peur de « GG. » (MPC 13-01-0242 s. et 13-01-0244). Il avait pu librement mettre un terme (provisoire) à son activité criminelle après sa prise d'emploi auprès de la société 11 (cf. ch. D.2.8 *supra* et MPC 13-01-0243 et 13-01-0277) mais « EE. » l'avait ensuite supplié de faire une dernière session avec lui et il avait fini par céder, après que « EE. » lui avait même envoyé la preuve d'un virement d'EUR 1 million pour l'appâter et lui montrer que les fraudes fonctionnaient toujours. Selon les premières déclarations du prévenu, c'était là, la raison pour laquelle il avait repris les fraudes en mai 2018 (MPC 13-01-0243). Ces premières déclarations paraissent crédibles et cohérentes. De surcroît, le prévenu a manifestement gardé des liens avec ses acolytes après sa prise d'emploi chez la société 11, ayant alors encore continué son activité criminelle avec eux pendant deux mois supplémentaires (cf. ch. D.2.8 *supra*). Ainsi, A. a bien gardé des liens avec ses acolytes et même continué à perpétrer des fraudes, même après avoir augmenté ses revenus de manière licite, grâce à un emploi chez la société 11. Il a agi de la sorte en étant principalement mu par l'appât du gain, tant aux mois de novembre et décembre 2017, qu'entre mai et juillet 2018.

Partant, la Cour considère que c'était bien toujours la perspective du lucre – et non, nouvellement, la peur – qui a amené A. à reprendre les fraudes en mai 2018 et qu'il a continué à agir sous l'effet d'une même volonté délictuelle originelle. Il n'y a dès lors pas lieu de considérer que le prévenu aurait agi, dès mai 2018, pour des motifs différents et ensuite d'une décision de passage à l'acte distincte, et qu'il aurait ainsi commis une nouvelle infraction, entraînant l'application d'un concours au sens de l'art. 49 al. 1 CP.

4.2.6 A. et ses acolytes ont cherché à obtenir les accès *e-banking* des sociétés dans le seul but de pouvoir procéder au débits frauduleux (dossier d'instruction *e contrario*). Si, par la connexion *e-banking*, ils ont pu prendre connaissance de données bancaires des sociétés, cette prise de connaissance servait *in fine* exclusivement à la commission des détournements de fonds (id.). En particulier, l'enquête n'a par exemple pas mis à jour que A. et ses acolytes auraient vendu les accès ou les données bancaires des sociétés, ou qu'ils les auraient autrement mis à disposition de tiers. Au contraire, les acolytes du prévenu ont immédiatement essayé de passer les ordres bancaires pour soustraire des avoirs et s'enrichir par une répartition du butin. Partant, il n'apparaît pas que les accès *e-banking* ou les données bancaires des sociétés aient présenté, pour le prévenu et ses acolytes, une valeur patrimoniale, ni que la soustraction de ces données ait résulté d'une démarche et volonté distincte des débits frauduleux. Il n'y a dès lors par lieu de s'écarter de la jurisprudence de la Cour de céans dans le cas d'espèce et la soustraction des accès *e-banking* et autres données bancaires doit être considérée comme absorbée par le chef d'infraction de l'art. 147 CP, sans que l'art. 143 CP s'applique en concours. L'accès indu à un système informatique (tel que réprimé par l'art. 143bis CP) est lui-même absorbé par la soustraction de données.

4.2.7 Partant, A. doit être condamné pour la seule utilisation frauduleuse d'un ordinateur par métier au sens de l'art. 147 al. 1 et 2 CP, l'ensemble des 23 cas, tentés et consommés, étant absorbés par la commission de cette infraction unique.

Il convient encore pour la Cour d'examiner si sa contribution doit être considérée comme celle d'un auteur principal ou A. a agi comme le complice de ses acolytes.

5. Degré de participation de A.

5.1 Est un participant principal à l'infraction celui dont la contribution est à tel point essentielle que, en fonction des circonstances du cas d'espèce et à la lumière du plan délictueux, l'exécution ou la non-exécution de l'infraction considérée en dépende, c'est-à-dire que son rôle soit plus ou moins indispensable à la réussite de l'entreprise. Contrairement au complice qui est un participant secondaire qui

prête assistance pour commettre un crime ou un délit, le coauteur est celui qui collabore, intentionnellement et de manière déterminante, avec d'autres personnes à la décision de commettre une infraction, à son organisation ou à son exécution, au point d'apparaître comme l'un des participants principaux. Il faut que, d'après les circonstances du cas concret, la contribution du coauteur apparaisse essentielle à l'exécution de l'infraction. La seule volonté quant à l'acte ne suffit pas. Il n'est toutefois même pas nécessaire que le coauteur ait effectivement participé à l'exécution de l'acte ou qu'il ait pu l'influencer. La coactivité suppose une décision commune, qui ne doit cependant pas obligatoirement être expresse, mais peut aussi résulter d'actes concluants, le dol éventuel quant au résultat étant suffisant. Il n'est pas nécessaire que le coauteur participe à la conception du projet, auquel il peut adhérer ultérieurement. Il n'est pas non plus nécessaire que l'acte soit prémédité ; le coauteur peut s'y associer en cours d'exécution. Ce qui est déterminant, c'est que le coauteur se soit associé à la décision dont est issue l'infraction ou à la réalisation de cette dernière, dans des conditions ou dans une mesure qui le font apparaître comme un participant non pas secondaire, mais principal (arrêts du Tribunal fédéral 6B_1044/2023 du 20 mars 2024, consid. 1.2.1 et 6B_1166/2023 du 13 juin 2024, consid. 1.2, et références citées). Une contribution fournie entre le commencement d'exécution d'une infraction et la consommation (formelle ; *Vollendung*) de celle-ci, voire son achèvement (matériel ; *Beendigung*), est toujours essentielle lorsque l'agent adopte tout ou une partie du comportement incriminé, au sens de la conception objective formelle de la participation principale (STRÄULI, in CR-CP, n° 99 et 105 ad introduction aux art. 24-27 CP). Dans l'hypothèse d'un délit élémentaire (*einaktiges Delikt*), caractérisé par l'unicité de l'agissement incriminé, l'exécution de ce dernier pourra être répartie sur plusieurs protagonistes. Face à un délit complexe (*mehraktiges Delikt*), l'accomplissement de l'un des actes réprimés suffira (STRÄULI, in CR-CP, n° 16 ad introduction aux art. 24-27 CP). Lorsque les éléments objectifs et subjectifs constitutifs de la coactivité sont réalisés, chaque protagoniste répond pour ce que les autres ont fait, comme s'il avait accompli lui-même l'ensemble des actes d'exécution de l'infraction considérée. Cette imputation réciproque des contributions des différents coauteurs rend sans objet la question de la causalité naturelle de chacun d'entre elles prise isolément (STRÄULI, in CR-CP, n° 108 ad introduction aux art. 24-27 CP et références citées).

Il existe un rapport de subsidiarité entre la complicité et la coactivité, en ce sens qu'une participation au stade de l'exécution de l'infraction ne fondera une complicité qu'à défaut d'avoir satisfait aux exigences de la coactivité (STRÄULI, in CR-CP, n° 10 ad art. 25 CP).

5.2 En l'espèce, la Cour a constaté que A. a, dans les 23 cas, exécuté la deuxième phase de la fraude (en collaboration directe avec « FF. »), à savoir celle consistant pour lui à contacter la société en se faisant passer pour un informaticien de la banque, amener son interlocuteur à se connecter à distance à l'ordinateur de « FF. » et, ainsi, obtenir les accès *e-banking* de la société (cf. ch. 4.2.1 *supra*). Le rôle effectivement joué par A. était indispensable à l'obtention des accès *e-banking* et, ainsi, condition *sine qua non* à l'exécution des débits frauduleux selon le *modus operandi* défini : la fraude nécessitait qu'il soit pris contact avec l'employé et que celui-ci soit convaincu d'exécuter le programme à distance et d'introduire les accès *e-banking* dans son ordinateur. La contribution du prévenu à la commission du crime était ainsi déterminante dans sa réalisation. Le prévenu a agi en connaissance du but de sa démarche – soit de passer des transactions indues grâce aux accès *e-banking* obtenus – et appelait de ses vœux la réalisation des fraudes, à laquelle il était personnellement intéressé. Il s'est non seulement associé à la décision de commettre ces fraudes, sur proposition de « EE. », mais a aussi apporté son concours à leur exécution en adoptant une partie du comportement réprimé par le chef d'utilisation frauduleuse d'un ordinateur (par métier), soit en obtenant (en collaboration directe avec « FF. ») les accès *e-banking* nécessaires à leur utilisation indue.

5.3 Les éléments relevés par la défense à cet égard ne sont pas pertinents. Le fait que le prévenu ne soit pas la seule personne à avoir exercé un rôle-clé dans l'exécution de ces fraudes et que « EE. », « FF. » ou « GG. » aient également apporté une contribution décisive à celle-ci ou l'ait favorisée n'a pas d'impact quant au caractère (lui aussi) déterminant de la contribution du prévenu (SK 37.721.089). Il en va de même de l'hypothèse selon laquelle le prévenu n'était pas irremplaçable et qu'il eut peut-être été possible à autrui d'effectuer, à la place de A., la part des démarches qui lui étaient dévolues (SK.721.090). C'est en effet le rôle du prévenu, soit l'exécution de la deuxième phase (en collaboration directe avec « FF. ») qui était, lui, fondamental et ainsi la contribution du prévenu, à la commission de l'infraction, l'était également. De surcroît, le prévenu a lui-même indiqué que la phase d'acquisition des accès *e-banking* nécessitait la coopération de deux personnes, soit de lui-même et « FF. » (cf. ch. D.2.4 *supra*). Enfin, la rémunération du prévenu démontre que de la perception-même des auteurs, son rôle n'était pas marginal ou celui d'un subalterne : « EE. », « FF. », « GG. » et le prévenu ont partagé équitablement leur part au butin de 45%, la rémunération légèrement supérieure revenant à « EE. » et « FF. », par 4.5% (10% x 45%), s'expliquant par des motifs objectifs, soit la mise à disposition de l'infrastructure, et étrangers à une hiérarchisation des protagonistes entre eux (cf. ch. D.2.6 *supra*).

5.4 Partant, la Cour constate que A. a agi comme coauteur des faits d'utilisation frauduleuse d'un ordinateur par métier dont il est reconnu coupable ce jour, et non comme un simple complice, au sens de l'art. 25 CP.

6. Conclusions sur les infractions

Il découle de ce qui précède que A. doit être reconnu coupable d'utilisation frauduleuse d'un ordinateur par métier (art. 147 al. 1 et 2 aCP) pour les faits décrits aux chiffres 1.3.1 à 1.3.23 de l'acte d'accusation. Il est en revanche acquitté des chefs d'accusation de soustraction de données (art. 143 CP), d'accès indu à un système informatique (art. 143bis CP) et d'utilisation frauduleuse d'un ordinateur (art. 147 CP) pour les faits décrits aux chiffres 1.3.24 et 1.3.25 de l'acte d'accusation.

7. Peine

7.1 Des principes de la fixation de la peine

7.1.1 Selon l'art. 47 CP, le juge fixe la peine d'après la culpabilité de l'auteur. Il prend en considération les antécédents et la situation personnelle de ce dernier ainsi que l'effet de la peine sur son avenir (al. 1). La culpabilité est déterminée par la gravité de la lésion ou de la mise en danger du bien juridique concerné, par le caractère répréhensible de l'acte, par les motivations et les buts de l'auteur et par la mesure dans laquelle celui-ci aurait pu éviter la mise en danger ou la lésion, compte tenu de sa situation personnelle et des circonstances extérieures (al. 2). La culpabilité de l'auteur doit être évaluée en fonction de tous les éléments qui ont trait à l'acte lui-même (*Tatkomponente*).

7.1.2 Parmi ceux-ci, il convient de distinguer les *Tatkomponente* objectifs et subjectifs ; font partie des premiers la gravité de la lésion, le caractère répréhensible de l'acte et son mode d'exécution (ATF 142 IV 137 consid. 9.1; 141 IV 61 consid. 6.1.1). S'agissant de la gravité de la lésion, on tiendra compte de l'importance du bien juridiquement protégé par la norme et du résultat de l'activité illicite (jugement de la Cour des affaires pénales SK.2020.23 du 20 juillet 2021, consid. 6.1.3).

7.1.3 Au chapitre des *Tatkomponente* subjectifs, il faut tenir compte de l'intensité de la volonté délictuelle ainsi que des motivations et des buts de l'auteur.

7.1.4 A ces composantes de la culpabilité, il convient, en outre, d'ajouter les facteurs liés à l'auteur lui-même (*Täterkomponente*), à savoir ses antécédents judiciaires et non-judiciaires, sa réputation, sa situation personnelle (état de santé, âge, obligations familiales, situation professionnelle, risque de récidive, etc.), sa

vulnérabilité face à la peine, de même que son comportement après l'acte et au cours de la procédure pénale (ATF 142 IV 137 consid. 9.1; 141 IV 61 consid. 6.1.1; jugement de la Cour des affaires pénales SK.2020.23 précité consid. 6.1.3).

7.2 De la gravité objective de l'acte

7.2.1 Au chapitre des *Tatkomponente* objectifs aggravant la culpabilité de A., la Cour relève en premier lieu le haut degré d'organisation et de préparation des auteurs. Ils se sont réparti les tâches aux fins de mener à bien les fraudes selon un procédé précis et détaillé, pour l'exécution duquel A. a dû s'entraîner en binôme avec « FF. » pendant plusieurs jours, afin de perfectionner leur réalisation de la deuxième phase (acquisition des accès *e-banking*). De plus, les sociétés visées ont été sélectionnées de manière à maximiser les chances de pouvoir procéder à un détournement de fonds important et le procédé des auteurs visait notamment à obtenir les informations nécessaires pour ce faire (obtention de renseignements sur les habitudes bancaires ; SK 37.731.013). La duperie utilisée par A. était élaborée : il a utilisé le prétexte d'une migration informatique pour tromper les sociétés lésées et obtenir leurs accès *e-banking*, en leur faisant craindre que si elles n'obtempéraient pas, leur accès seraient coupés (id.). Afin de renforcer la confiance des employés et maintenir son emprise sur ceux-ci, le prévenu a usé tour à tour de séduction, en feignant la bonhommie, puis menacer les employés de conséquences graves si ceux-ci consultait leur *e-banking* (id). Ces menaces visaient uniquement à éviter que les sociétés découvrent à temps la fraude pour récupérer les fonds débités (id). Ainsi, A. et ses comparses ont usé ensemble de procédés raffinés, nécessitant un haut degré de coordination et une préparation et exécution soigneuses.

7.2.2 En second lieu, la Cour relève l'absence totale de scrupule du prévenu. A. a multiplié les appels ; il les chiffre à plusieurs centaines (MPC 13-01-0272). Il a, de concours avec ses coauteurs, prélevé des montants conséquents sur les comptes des sociétés lésées, tendant à dessein à maximiser le butin. Dans la moitié des 30 versements, les ordres de transfert portent sur des sommes allant de CHF 100'000.- à CHF 200'000.-. Dans l'autre moitié des cas, ce sont des montants allant de CHF 200'000.- à CHF 1'000'000.- dont les auteurs ont ordonné le transfert. D'ailleurs, A. a expliqué qu'ils avaient « eu le trac » lorsqu'il était à prévoir que les comptes de la société devaient être particulièrement bien fournis (MPC 13-01-0264). A. et ses coauteurs n'ont ainsi eu aucun égard pour les sociétés lésées et les difficultés financières dans lesquelles ils les plongeaient par leurs agissements ou le tort énorme qu'ils causaient aux employés dont le prévenu abusait de la confiance : seul le butin comptait à leurs yeux. D'ailleurs, lorsque confronté à ses agissements par des sociétés lésées, le prévenu n'a pas hésité à user d'excuses et de reproches pour les rassurer, aux fins d'éviter

qu'elles se rendent compte à temps des fraudes (cf. ch. E.2.2 *supra* et SK 37.731.014).

7.2.3 En troisième lieu, la Cour relève l'absence de pitié du prévenu. Il ressort des enregistrements qu'il adopte une attitude parfois ouvertement moqueuse vis-à-vis des employés, sans utilité pour parvenir à ses fins criminelles, voire contreproductives à celles-ci. Ainsi, par exemple, lors de l'appel ID1000048614717, le prévenu met son interlocutrice sur hautparleur alors qu'elle tient des propos gênants (2:32). Lors d'un autre appel, il met aussi son interlocutrice sur hautparleur et lui passe un film pornographique (cf. ch. P.2.3 *supra*). Ces agissements sont l'expression du mépris du prévenu à l'égard de ses victimes. Non content de délester les sociétés visées de sommes importantes, causant aussi un tort très important aux employés qu'il trompait, le prévenu s'est encore permis des plaisanteries à leur dépend.

7.2.4 En quatrième lieu, la Cour relève que le prévenu et ses coauteurs ont passé des débits frauduleux pour un montant total d'environ CHF 9 millions, dont des ordres d'environ CHF 5 millions ont été exécutés. Au-delà du caractère durable de ces agissements, tendant à la perception de revenus réguliers – qui relèvent de l'aggravante du métier – l'intensité de l'activité délictuelle déployée par les auteurs a porté une atteinte conséquente aux intérêts patrimoniaux des sociétés, respectivement leur mise en danger.

7.2.5 Dès lors que le métier (au sens de l'art. 147 al. 2 CP) s'applique, il n'y a pas lieu pour la Cour de retenir comme facteur aggravant la longue période d'activité criminelle du prévenu (une demi-année répartie sur 20 mois), ni son enrichissement personnel conséquent de EUR 24'523.-/mois, qui sont déjà compris dans cette qualification.

7.2.6 Enfin, au chapitre des *Tatkomponente* objectifs, la Cour relève que les auteurs ont visé des personnes morales et non des personnes physiques faibles ou aux capacités diminuées, à l'instar des fraudes commises au préjudice de personnes âgées, par exemple. Cela étant, le fait de n'avoir démarché que des sociétés relève du *modus operandi* et, *in fine*, d'une recherche de maximisation des gains criminels, et non d'une volonté d'épargner des victimes présumées faibles. A cela s'ajoute que les auteurs ont ciblé des sociétés suisses déployant pour la plupart une activité internationale, ce qui leur permettait de procéder plus facilement à des débits importants vers l'étranger, tout en diminuant le risque que ces transactions ne soient découvertes ou bloquées dans le contexte de la vigilance bancaire.

7.2.7 Ainsi, la gravité de la faute objective doit être qualifiée de moyenne. Si, par hypothèse, d'autres affaires d'utilisation frauduleuse d'un ordinateur par métier peuvent être qualifiées de plus graves, notamment en raison de l'ampleur et de

la durée de l'activité criminelle, du nombre de fraudes commises et du butin obtenu, la Cour estime que la gravité objective des faits dont le prévenu s'est rendu coupable dépasse très clairement le cadre d'une affaire de faible gravité.

7.2.8 Cette gravité objective des faits est entièrement imputable à A., qui connaissait la répartition interne des tâches et le *modus operandi*, les ayant d'ailleurs lui-même expliqués aux autorités. Le prévenu était parfaitement informé du mécanisme criminel utilisé. De plus, c'est lui qui a trompé les employés pour obtenir les accès *e-banking* des sociétés. Il connaissait le montant des transactions, qui lui était communiqué par « EE. », y compris lorsque le montant avait par la suite été bloqué par la banque. Le prévenu percevait sa part du butin quelques jours après le détournement de fonds (MPC 13-01-0276). Il se tenait ainsi informé des résultats des détournements opérés. Par ses agissements, le prévenu a cherché à s'enrichir pour maintenir un train de vie fastueux. Il a même poursuivi ses activités délictuelles en novembre et décembre 2017, puis les a reprises en mai 2018, alors qu'il n'avait plus besoin de commettre des fraudes pour assurer son train de vie, vu qu'il avait pris un emploi chez la société 11 le 1er novembre 2017. Il a ainsi agi par dol direct, en pleine connaissance de cause et de manière délibérée.

7.3 <u>De la gravité subjective de l'acte</u>

7.3.1 Au chapitre des *Tatkomponente* subjectifs aggravants, la Cour relève que A. a dépassé ses scrupules initiaux et – après réflexions (« j'ai beaucoup réfléchi ») – a décidé de s'adonner à une activité criminelle pour assouvir des envies purement superficielles, soit l'achat d'habits et des voyages (cf. ch. D.2.6 s. *supra* et SK 37.731.010). Selon le prévenu, il a consommé l'ensemble de ses revenus criminels pour ce genre de divertissements, outre le paiement de 10% en faveur d'œuvres caritatives, conformément à des exigences religieuses (id.). Pourtant, parallèlement, le prévenu gagnait sa vie par des activités licites et percevait des revenus mensuels d'ILS 25'000.- à ILS 30'000.- (soit entre CHF 6'250.- et CHF 7'500.- ; SK.37.731.004), qu'il a encore augmentés par son activité chez la société 11 dès novembre 2017. Vu l'usage qu'il a fait de ses revenus d'origine criminelle, le prévenu n'avait manifestement pas besoin de ceux-ci pour subvenir aux besoins de sa famille, contrairement à ce qu'il a affirmé. En outre, même s'il a tenté de se justifier en évoquant les difficultés financières rencontrées dans son enfance, il n'en reste pas moins qu'il a agi pour assouvir ses propres plaisirs personnels, de manière purement égoïste. Fort de sa situation financière confortable, il aurait pu facilement, en raison de ses scrupules, refuser l'offre de « EE. » et renoncer à toute activité criminelle. Le mobile purement égoïste dont il a fait preuve aggrave dès lors légèrement sa faute.

7.3.2 La Cour constate ensuite que l'énergie criminelle déployée par A. est marquée. Il s'est d'abord entraîné avec « FF. » pour perfectionner son exécution des appels. Il a ensuite exécuté des centaines d'appels, ce qui a dû lui prendre une part non négligeable de son temps, étant précisé que ses agissements criminels ont duré au moins 6 mois. Durant cette période, il s'est installé dans la délinquance et ses agissements criminels sont devenus son mode de vie. Cela étant, ces facteurs ayant déjà été pris au compte au chapitre de la qualification aggravante du métier, l'énergie criminelle déployée par A. ne doit pas être prise en compte une nouvelle fois comme facteur aggravant au stade de l'examen de la gravité subjective des faits.

7.3.3 Enfin, il sied de relever que A. n'a, dans aucun des 23 cas dont il est reconnu coupable, renoncé à poursuivre la commission de l'infraction ou contribué à empêcher sa consommation (art. 22 al. 1 et 23 CP). Ce sont toujours des facteurs externes et indépendants de sa volonté qui ont interrompu le cours de celle-ci (i.e. impossibilité d'établir l'accès à distance ou blocage de la transaction par les banques). S'agissant du cas de la société 8, A. a précisé aux débats qu'il n'avait précisément pas interrompu le cas de son propre chef, mais sur signe de la main de « FF. » (cf. ch. Y.2.2 *supra*).

Partant, la Cour constate l'absence de tout facteur d'atténuation de la gravité subjective de l'acte.

7.3.4 Au vu de ce qui précède, la gravité de la faute subjective doit aussi être qualifiée de moyenne.

7.4 <u>De la peine hypothétique</u>

7.4.1 L'utilisation frauduleuse d'un ordinateur par métier au sens des art. 147 al. 1 et 2 aCP est réprimée d'une peine privative de liberté de 10 ans au plus ou d'une peine pécuniaire de 90 jours-amende au moins. Depuis le 1er juillet 2023, cette infraction est sanctionnée d'une peine privative de liberté de 6 mois à 10 ans.

7.4.2 La gravité objective et subjective des faits est moyenne (cf. ch. 7.2 et 7.3 *supra*). Partant, la Cour fixe la peine privative de liberté hypothétique à 60 mois pour l'infraction d'utilisation frauduleuse d'un ordinateur par métier.

7.4.3 Il convient ensuite d'examiner si des facteurs liés à l'auteur (*Täterkomponente*) aggravent ou atténuent la peine hypothétique.

7.5 Des facteurs liés à l'auteur

7.5.1 La situation personnelle du prévenu se présente comme suit :

A. est aujourd'hui âgé de 37 ans. Il est de nationalité française et israélienne. Né en France, il y a vécu jusqu'à son émigration en Israël, au début de l'adolescence (« j'ai fait jusqu'à ma sixième en France » ; SK 37.731.002). Le prévenu est marié et père de quatre enfants (SK 37.231.4.007). En raison de ses difficultés scolaires de nature linguistique en Israël, le prévenu n'y a pas obtenu son certificat de fin de scolarité obligatoire à l'issue de celle-ci. Il a ensuite travaillé notamment comme DJ, graphiste et dans le domaine des assurances. Aujourd'hui, il est employé comme technicien par la société 11, pour laquelle il effectue des installations de téléphonie, d'internet et de télévisions. A. travaille également pour le magasin de la société 36, dans le domaine fournisseurs (SK 37.731.003).

Cumulées, les activités de A. représentent un travail à temps plein et il perçoit des revenus d'ILS 22'000.-, nets d'impôts et de charges sociales, soit environ CHF 5'500.- par mois. L'épouse du prévenu ne travaillait pas au moment des faits. L'année dernière, elle a pris une activité professionnelle à temps partiel comme comptable et perçoit un salaire d'ILS 13'000.-, soit environ CHF 3'250.- par mois, également net d'impôts et de charges sociales (SK 37.731.004 et 37.731.006). Les charges du ménage de A. sont composées des dépenses du quotidien (nourriture, habits, scolarité des enfants, etc.), des coûts de l'assurance-maladie à raison d'ILS 600.- par mois et d'une dette hypothécaire dont le remboursement et les intérêts se chiffrent à ILS 18'000.- par mois (SK 37.731.006 et 37.731.009).

Le prévenu est propriétaire de deux appartements de cinq pièces chacun, à Netanya (IL) (SK 37.731.004 s.), d'une valeur d'ILS 4 millions (CHF 1 million) par appartement (SK 37.731.0008). La dette hypothécaire pour les deux appartements s'élève actuellement à ILS 3 millions. A. a acheté le premier de ces biens immobiliers en 2014 ou 2015 et le second en 2016 (MPC 13-01-0021 et SK 37.731.007). Le prévenu habite l'un des appartements avec sa famille, l'autre logement est vide (SK 37.731.027).

La situation personnelle de A. et l'effet de la peine sur son avenir ont un effet neutre sur la peine devant être prononcée ce jour, étant rappelé que ce n'est qu'en présence de circonstances extraordinaires que le tribunal peut atténuer la peine à ce titre. S'agissant en particulier de la présence d'enfants en bas âge, la jurisprudence retient que l'auteur d'infractions doit en principe prévoir et assumer les conséquences de son incarcération sur sa famille. A titre extraordinaire, elle a par exemple admis une circonstance légèrement atténuante dans une affaire relative à l'incarcération d'une mère élevant seule ses enfants qui devaient dès lors être placés hors du noyau familial (arrêt du Tribunal fédéral 6B_312/2016 du

23 juin 2016, consid. 1.5.3 et références citées). Le cas d'espèce n'est pas comparable. A. n'élève pas seul ses enfants mais avec son épouse, leur mère. Jusqu'à peu, cette dernière se consacrait entièrement à sa vie de famille et n'a repris que récemment une activité professionnelle à temps partiel. Bien que l'impact d'une incarcération de A. sur sa vie de famille ne soit pas à nier, sa situation personnelle n'est pas extraordinaire à ce titre.

7.5.2 A teneur de ses casiers judiciaires suisse et français, A. n'a pas d'antécédent judiciaire. La Cour n'a pas reçu des autorités israéliennes le casier judiciaire du prévenu dans ce pays. Selon le prévenu, il n'aurait pas d'antécédent en Israël non plus (SK 37.731.006). La Cour constate dès lors l'absence d'antécédent, ce qui a un effet neutre sur la peine devant être prononcée ce jour.

7.5.3 Le prévenu n'a pas entrepris de démarche en faveur des société lésées pour les rembourser, alors qu'il est le propriétaire de deux appartements financés par des fonds propres à hauteur d'ILS 1 million (cf. ch. 7.5.1 *supra* et SK 37.731.023). Aux débats, il a affirmé n'avoir pas vendu son deuxième appartement – qui est pourtant vide – en raison de la chute des prix de l'immobilier après le début de la guerre à Gaza (SK 37.731.027). Or, le conflit auquel le prévenu fait référence a notoirement débuté le 7 octobre 2023, soit près de 10 mois après la libération du prévenu de détention provisoire, le 14 décembre 2022. A. aurait donc disposé de tout le temps nécessaire pour entreprendre ne serait-ce que de premières démarches afin de libérer des liquidités, en particulier en vendant son appartement vide, et essayer de rembourser aux sociétés lésées une partie de leur préjudice. Il n'a d'ailleurs pas non plus pris contact avec les sociétés pour au moins leur présenter directement ses excuses ou proposer un plan de remboursement (SK 37.731.25). Ainsi, le prévenu n'a pas manifesté de repentir sincère par ses actes, au sens de l'art. 48 let. d CP, et aucune circonstance atténuante ne peut être retenue à ce titre.

7.5.4 La Cour retient en revanche l'écoulement du temps comme circonstance atténuante dans le cas d'espèce (art. 48 let. e CP). En effet, le prévenu a débuté ses activités criminelles au mois de décembre 2016, soit près de 8 ans et demi avant le prononcé du présent jugement. A. ne semble pas avoir commis de nouvelles infractions depuis qu'il a arrêté de participer aux fraudes objet de la présente procédure, en juillet 2018. L'infraction en cause était de nature patrimoniale et n'attentait pas à des biens juridiques supérieurs. Certes les deux tiers du délai de prescription de 15 ans (97 al. 1 let. b CP) ne sont pas encore atteints, étant rappelé que celui-ci a commencé à courir avec la commission du dernier cas, le 30 juillet 2018 (cf. ch. Z.1 *supra*). Toutefois, cela fait près de 7 ans que le prévenu a arrêté son activité criminelle, dont le début remonte, comme mentionné, à il y a environ 8 ans et demi. Selon la jurisprudence, si un motif d'atténuation de la peine doit dans tous les cas être retenu lorsque les deux tiers du délai de prescription sont écoulés, le juge peut réduire cette durée et admettre

une circonstance atténuante avant qu'elle soit atteinte, afin de tenir compte de la nature et de la gravité de l'infraction (ATF 140 IV 145 consid. E.3.1 et 132 IV 1 consid. 6.2). La Cour considère que tel est le cas en l'espèce et que la peine hypothétique doit dès lors être réduite de 3 mois.

7.5.5 La Cour retient encore que A. a, dans une certaine mesure, avoué les faits et coopéré avec les autorités. Cette coopération n'est cependant pas pleine et entière et elle doit être relativisée. En effet, ce n'est que près de 9 mois après son arrestation et pas moins de 7 auditions, lors desquelles il a invariablement prétendu ne pas être impliqué dans les faits sous enquête, que A. s'est décidé à s'expliquer. A ce moment-là, l'enquête avait déjà permis de collecter un nombre important de moyens de preuve et une analyse comparative de voix, à charge. De plus, même après avoir annoncé vouloir s'expliquer, A. n'a pas été entièrement transparent avec les autorités. Il a, par exemple, encore prétendu ne pas être impliqué dans le cas C., ce qu'il a par la suite dû admettre être faux. Néanmoins, le prévenu a fourni aux enquêteurs de nombreux détails quant à la répartition des tâches avec « GG. », « FF. » et « EE. » et à celle du butin. La Cour prend donc en considération une certaine coopération à l'avancement de l'enquête et cette circonstance entraîne une atténuation supplémentaire de la peine hypothétique par 9 mois.

Par contre, la présence aux débats du prévenu a un effet neutre sur sa peine. Il est rappelé que A. s'était engagé à se présenter et à rester à la disposition des autorités pénales suisses, dans le contexte de sa libération sous caution. Sa présence aux débats était ainsi l'une des conditions au prononcé de cette mesure de substitution à la détention (cf. ch. A.4 *supra*).

7.5.6 Les menaces alléguées par A., qui auraient commencé après sa libération de détention provisoire, n'ont pas non plus un effet atténuant sur la peine. D'une part, il n'est pas établi que ces menaces soient en lien avec la commission des infractions dont la présente procédure fait l'objet (SK 37.731.017). Même si tel devait être le cas, elles ne constitueraient pas encore une conséquence directe de l'infraction commise par A., en elle-même (au sens de l'art. 54 CP), mais tout au plus de ses associations peu recommandables avec sa connaissance « GG. » (MPC 13-01-0240 et 13-01-0243). De surcroît, les craintes que ces menaces auraient inspirées à A. ne sont pas d'une intensité suffisante pour retenir un effet atténuant. A. dit certes avoir quitté son domicile pendant trois semaines. Il y est toutefois revenu et a depuis repris sa vie à Netanya (IL) (SK 37.731.017 et 37.731.028 s.).

7.5.7 Enfin, la Cour constate qu'il n'y a pas eu violation du principe de célérité. En effet, la PJF a rendu son rapport final en mars 2023, ensuite de quoi l'avis de prochaine clôture a été envoyé aux parties en novembre 2023. Les débats de première instance se sont tenus environ une année après la saisine de la Cour, ce qui

n'apparaît pas particulièrement long au vu du volume du dossier dont il a fallu prendre connaissance. Partant, la Cour ne constate aucun motif d'atténuation de la peine à ce titre.

7.6 De la fixation de la peine

7.6.1 Comme exposé ci-avant, la peine hypothétique de 60 mois doit être atténuée à raison de 12 mois (3 mois + 9 mois), pour tenir compte de l'écoulement du temps et de la collaboration de A. à l'enquête. Il y a lieu d'en déduire intégralement la détention provisoire, y compris la détention extraditionnelle, subie par le prévenu entre le 31 janvier 2022 et le 14 décembre 2022 (art. 51 CP).

7.6.2 Ainsi, la Cour condamne A. à une peine privative de liberté de 48 mois (60 mois – 12 mois), sous déduction de la détention avant jugement subie, soit 318 jours.

7.6.3 Au vu des conclusions prises par Me Sébastien Fanti et Me Miriam Mazou à cet égard aux débats, il est relevé que la partie plaignante ne peut interjeter recours sur la question de la peine ou de la mesure prononcée (art. 382 al. 2 CPP). Il lui est toutefois loisible de mettre en exergue les éléments en fait qui, selon elle, démontrent ou aggravent la faute, et de les plaider. Par ailleurs, la Cour doit, matériellement, traiter de la peine dans son jugement. Partant, il n'y a pas lieu de prononcer une non-entrée en matière sur la conclusion de Me Sébastien Fanti quant à la peine, comme requis par Me Miriam Mazou.

7.7 De la licéité des conditions de détention

7.7.1 A. a été détenu du 20 avril au 2 juin 2022 à la prison T., soit durant 44 jours (SK 37.262.1.005). Il y a partagé sa cellule avec un codétenu. La cellule présentait une surface de 12 m^2, dont 1.5 m^2 pour les sanitaires (SK 37.262.1.003). La surface nette par détenu était donc de 5.25 m^2 ([12 m^2 - 1.5 m^2] / 2). La cellule disposait en outre d'un système d'aération et les sanitaires étaient séparés du reste de la cellule par un rideau (SK 37.262.1.003). Le prévenu n'a pas eu l'occasion de travailler et n'a participé à aucune activité socio-éducative. Il a toutefois bénéficié de 1.5 heure de sport par semaine, d'une heure de promenade quotidienne et de visites (10 visites d'au moins une heure chacune), en sus de deux auditions (SK 37.262.1.004 et 37.262.1.007).

7.7.2 La détention de A. à la prison AA. a duré du 2 juin au 14 décembre 2022.

7.7.3 Du 2 juin au 19 octobre 2022, soit durant 140 jours, il y a occupé une cellule de 11.61 m^2, dont 1.5 m^2 pour les sanitaires, avec un codétenu (SK 37.262.2.003, 37.262.2.005 ss et 37.262.2.017). La surface nette par détenu était donc de 5.06 m^2 ([11.61 m^2 - 1.5 m^2] / 2). La cellule disposait, en outre de la fenêtre, d'un ventilateur et les sanitaires étaient séparés du reste de la cellule par un rideau.

Le prévenu n'a pas eu l'occasion de travailler mais a toutefois bénéficié de quatre séances de sport par semaine et d'une heure de promenade par jour. Il a également pu participer à des activités socio-éducatives et se rendre à la bibliothèque (SK 37.262.2.004).

7.7.4 Du 19 octobre au 14 décembre 2022, soit durant 57 jours, le prévenu a occupé une cellule de 9.68 m^2, dont 1.5 m^2 pour les sanitaires, avec un codétenu (SK 37.262.2.003, 37.262.2.005 ss et 37.262.2.017). La surface nette par détenu était donc de 4.09 m^2 ([9.68 m^2 -1.5 m^2] / 2). Cette cellule disposait aussi d'un ventilateur et d'un rideau séparant les sanitaires du reste de la surface. Durant cette période, A. a bénéficié d'une activité à l'intendance (trois jours de travail durant six semaines, puis quatre jours de travail durant six semaines, à raison de 70%). Il s'acquittait de ses tâches en alternance avec son codétenu, de sorte qu'il a bénéficié de l'entier de la cellule pendant que son codétenu travaillait. En outre, il a bénéficié d'une heure de promenade par jour et de trois séances de sport de 45 minutes par semaine (SK 37.262.2.004).

7.7.5 Le prévenu a bénéficié de 54 visites au total pendant sa période de détention à la prison AA. (SK 37.262.2.004).

7.7.6 Il ne ressort pas de ce qui précède que A. aurait été détenu dans des conditions illicites. D'ailleurs, aucune conclusion en la matière n'a été prise par le prévenu.

8. Expulsion

8.1 A. dispose des nationalités française et israélienne. Se pose dès lors la question du prononcé de son expulsion.

8.2 Aux termes de l'art. 66*a* al. 1 CP, le juge expulse de Suisse pour une durée de 5 à 15 ans l'étranger condamné pour l'une des infractions figurant dans ledit alinéa, quelle que soit la quotité de la peine prononcée à son encontre. Il peut exceptionnellement renoncer à l'expulsion obligatoire au sens de l'alinéa 1 lorsque celle-ci mettrait l'étranger dans une situation personnelle grave et que les intérêts publics à l'expulsion ne l'emportent pas sur l'intérêt privé de l'étranger à demeurer en Suisse (art. 66*a* al. 2 CP, 1ère phrase ; clause de rigueur). A cet égard, il tiendra compte de la situation particulière de l'étranger qui est né ou qui a grandi en Suisse.

8.3 Seule la commission par l'étranger de l'une ou l'autre des infractions répertoriées à l'alinéa 1 de l'art. 66*a* CP entraîne l'expulsion obligatoire de l'étranger qui les a perpétrées. Fait notamment partie du catalogue d'infractions de l'art. 66*a* al. 1 CP, le chef d'utilisation frauduleuse d'un ordinateur par métier au sens de l'art. 147 al. 2 CP (art. 66a al. 1 let. c CPP).

8.4 A. n'a aucun lien avec la Suisse. Il n'y a jamais séjourné (sauf pour les besoins de la présente procédure) et aucun de ses proches n'y vit (SK 731.021.024).

Dans ces conditions, il y a lieu de prononcer l'expulsion et de fixer sa durée selon la culpabilité du prévenu et le danger qu'il représente pour l'ordre et la sécurité publics suisses.

8.5 Domicilié à l'étranger, d'où il a perpétré les méfaits pour lesquels il est condamné ce jour, et ne présentant aucun lien avec la Suisse, où il ne s'était jamais rendu avant les débats dans la présente procédure, A. ne présente pas de danger particulier pour l'ordre public suisse. Il n'est pas à craindre qu'il pourrait à l'occasion d'une éventuelle future présence sur le territoire suisse – très théorique à ce stade – commettre de nouvelles infractions dans notre pays. Il y a dès lors lieu de fixer la durée de l'expulsion, obligatoire, au minimum de 5 ans.

8.6 Partant, la Cour prononce l'expulsion de A. pour une durée de 5 ans.

A. disposant de la nationalité française, l'expulsion n'est pas à inscrire dans le Système d'information Schengen (SIS).

9. Autorité d'exécution

9.1 Conformément à l'art. 74 al. 2 LOAP, l'autorité pénale de la Confédération désigne dans son prononcé le canton compétent en matière d'exécution, en application des art. 31 à 36 CPP. En cas d'infractions commises à l'étranger, ce sont les autorités du canton ayant demandé l'extradition qui sont compétentes, lorsque le prévenu n'a ni domicile, ni résidence, ni lieu d'origine en Suisse et qu'il n'a pas été appréhendé sur le territoire suisse (art. 32 al. 3 CPP).

9.2 En l'espèce, l'instruction, y compris la demande d'extradition, a été diligentée par le MPC depuis son site de Lausanne, c'est le Tmc VD qui a été saisi de toutes les demandes en matière de détention. C'est également dans le canton de Vaud que A. a été placé en détention provisoire.

9.3 Partant, les autorités du canton de Vaud sont compétentes pour l'exécution de la peine privative de liberté et de l'expulsion.

10. Sûretés

10.1 En présence d'un danger de fuite, le tribunal peut astreindre le prévenu au versement d'une somme d'argent afin de garantir qu'il se présentera aux actes de procédure et qu'il se soumettra à l'exécution d'une sanction privative de liberté (art. 238 al. 1 CPP). A teneur de l'art. 239 al. 1 CPP, les sûretés sont libérées dès que le motif de détention a disparu (let. a), la procédure pénale est close par une ordonnance de classement ou un acquittement entré en force (let. b) ou le prévenu a commencé l'exécution de la sanction privative de liberté (let. c).

10.2 En l'espèce, A. a été placé en détention provisoire pour risque de fuite, puis soumis à des mesures de substitution par ordonnance du Tmc VD du 12 décembre 2022. Par celles-ci, il a notamment été astreint au versement de sûretés par CHF 250'000.-. Il s'est en outre engagé à rester à la disposition des autorités pénales suisses et élire un domicile de notification en l'étude de son avocat (cf. ch. A.4 *supra*). A. est condamné ce jour à une peine privative de liberté (ferme) de 48 mois, sous déduction de la détention avant jugement subie par 318 jours, soit une peine d'emprisonnement sensible. Force est de constater que le risque de fuite n'a dès lors pas diminué depuis le prononcé des mesures de substitution, au contraire. De surcroît, le prévenu n'a pas encore commencé à purger le solde de sa peine, qui est supérieur à 36 mois. Ainsi, les conditions d'une libération des sûretés ne sont pas remplies (art. 239 al. 1 CPP) et il y a donc lieu de les maintenir en vue de l'exécution de la peine.

10.3 Partant, la Cour prononce le maintien des sûretés de CHF 250'000.- (état au 31.12.2024: CHF 252'966.05) déposées sur le compte du Ministère public de la Confédération auprès du Département fédéral des finances, selon la décision du 12 décembre 2022 du Tmc VD (réf. PC22.022533-CPB), pour garantir l'exécution de la peine privative de liberté prononcée à l'encontre de A.

11. Actions civiles

11.1 Droit applicable

11.1.1 Selon l'art. 122 al. 1 CPP, en qualité de partie plaignante, le lésé peut faire valoir des conclusions civiles déduites de l'infraction par adhésion à la procédure pénale. Les conclusions civiles consistent principalement en des prétentions en dommages-intérêts (art. 41 ss CO) et en réparation du tort moral (art. 47 et 49 CO) dirigées contre le prévenu (JEANDIN/FONTANET, Commentaire romand du Code de procédure pénale, 2ème éd. 2019 [ci-après : CR-CPP], n 16 s. ad art. 122 CPP et les références citées). Quoique régi par les art. 122 ss CPP, le procès civil dans le procès pénal demeure soumis à la maxime des débats et à la maxime de disposition. Ainsi, l'art. 8 CC est applicable au lésé qui fait valoir

des conclusions civiles déduites de l'infraction par adhésion à la procédure pénale (arrêt du Tribunal fédéral 6B _193/2014 du 21 juillet 2014, consid. 2.2 et les arrêts cités). Ces exigences se retrouvent à l'art. 123 al. 1 CPP, lequel impose au lésé de chiffrer ses conclusions civiles, de les motiver par écrit et de citer les moyens de preuve qu'il entend invoquer. S'agissant du devoir de motiver, il impose au lésé d'exposer les faits sur lesquels se fondent ses conclusions. Il s'agit non seulement des faits sur lesquels porte l'instruction relative à l'action pénale, mais aussi ceux permettant d'établir la quotité du dommage et le lien de causalité avec l'infraction poursuivie (JEANDIN/FONTANET, CR-CPP, n°5 ad art. 123 CPP et les références citées). Le calcul et la motivation des conclusions civiles doivent être présentés dans le délai fixé par la direction de la procédure conformément à l'art. 331 al. 1 CPP (art. 123 al. 2 CPP). Sur le plan procédural, la compétence pour juger des prétentions civiles appartient au tribunal saisi de la cause pénale, indépendamment de la valeur litigieuse (art. 124 al. 1 CPP). Le tribunal statue sur les conclusions civiles lorsqu'il rend un verdict de culpabilité à l'encontre du prévenu ou lorsqu'il l'acquitte et que l'état de fait est suffisamment établi (art. 126 al. 1 CPP). En revanche, il renvoie la partie plaignante à agir par la voie civile lorsqu'elle n'a pas chiffré ses conclusions de manière suffisamment précise ou ne les a pas suffisamment motivées (art. 126 al. 2 let. b CPP). L'art. 126 al. 2 let. b CPP constitue le pendant des exigences imposées par la loi à la partie plaignante relativement au calcul et à la motivation des conclusions civiles, et le non-respect de ces exigences conduit au renvoi de la partie plaignante à agir par la voie civile (JEANDIN/FONTANET, CR-CPP, n° 21 ad art. 126 CPP et les références citées).

11.1.2 Aux termes de l'art. 41 al. 1 CO, celui qui cause, d'une manière illicite, un dommage à autrui, soit intentionnellement, soit par négligence ou imprudence, est tenu de le réparer. Les quatre conditions suivantes doivent être réalisées : un acte illicite, une faute de l'auteur, un dommage et un rapport de causalité (naturelle et adéquate) entre l'acte fautif et le dommage (ATF 132 III 122 consid. 4.1).

11.1.3 Lorsque plusieurs [participants à un acte illicite] ont causé ensemble un dommage, ils sont tenus solidairement de le réparer, sans qu'il y ait lieu de distinguer entre l'instigateur, l'auteur principal et le complice (art. 50 al. 1 CO).

11.2 <u>Des prétentions civiles de B.</u>

11.2.1 Me Sébastien Fanti requiert au nom de B. la condamnation de A. au paiement des sommes de CHF 990'097.40 avec intérêts à 5% l'an dès le 27 janvier 2017, CHF 891.- avec intérêts à 5% l'an dès le 12 juin 2017 et CHF 45'407.85 avec intérêts à 5% l'an dès le 7 août 2017. Subsidiairement, la société conclut à la condamnation de A. au paiement des sommes de CHF 364'775.42 avec intérêts à 5% l'an dès le 27 janvier 2017, EUR 574'492.74 avec intérêts à 5% l'an dès le

27 janvier 2017, CHF 891.- avec intérêts à 5% l'an dès le 12 juin 2017 et CHF 45'407.85 avec intérêts à 5% l'an dès le 7 août 2017. Le tout sous suite de frais et dépens.

11.2.2 En premier lieu, la société B. demande la compensation de son dommage résultant directement des débits frauduleux (fonds détournés).

A. est condamné ce jour pour avoir participé au cas concernant la société B. (illicéité de l'acte et faute). Il a pu être établi que, dans ce contexte, ce sont des montants totaux de EUR 772'098.- et CHF 722'151.- qui ont été détournés de ladite société (cf. ch. J.2 *supra ;* dommage et lien de causalité). Une partie de ces fonds ont pu être bloqués et ont d'ores et déjà été restitués à B. (cf. ch. A.9 *supra*). Ainsi, le préjudice de B. s'élève à ce jour à EUR 574'492.74 (EUR 772'098.- - EUR 197'605.26) et CHF 364'775.42 (CHF 722'151.- - CHF 357'375.58). La société B. requiert le prononcé d'un intérêt de 5% l'an à compter du 31 janvier 2017, soit la date du dernier virement (art. 104 CO).

Dûment établies, les prétentions subsidiaires de B. en remboursement de son dommage (résiduel) résultant directement des débits frauduleux sont admises et A. est condamné au paiement, en mains de B., de EUR 574'492.74 et CHF 364'775.42, avec un intérêt de 5% l'an à compter du 31 janvier 2017.

11.2.3 En second lieu, B. demande le remboursement de certains frais du personnel.

En effet, ensuite des agissements de A., le responsable des finances de la société aurait été licencié, ce qui aurait occasionné des frais par CHF 891.- pour la mise au concours du poste, soit la publication d'une annonce sur un site dédié.

La Cour constate que le lien de causalité entre les agissements du prévenu et la nécessité de trouver un remplaçant au responsable des finances, respectivement la publication de l'annonce, n'est pas établi à suffisance de droit. En particulier, le licenciement du responsable des finances et les motifs qui ont sous-tendu celui-ci n'ont pas été démontrés.

Partant, la société B. est renvoyée à agir par la voie civile s'agissant de cette prétention (art. 126 al. 2 let. b CPP).

11.2.4 Enfin, la société B. demande le remboursement des frais engendrés par le remplacement de sa comptable, tombée en incapacité de travail pour dépression, ensuite de la fraude au préjudice de la société. A l'appui de sa demande, B. a produit des factures émanant de l'agence de placement 37 pour la location des services d'une personne durant les semaines 8 à 24 de l'année 2017, soit du 20 février 2017 au 18 juin 2017, soit CHF 45'407.85.

La Cour constate que le lien de causalité entre ces frais et les agissements de A. n'a pas non plus été démontré. Ainsi, il n'est pas possible de déterminer en quoi consistent les services de location fournis par l'agence de placement 37 et si ceux-ci découlaient des agissements du condamné. Ni le contrat de travail de la comptable, ni un certificat médical n'ont été versés. On ne sait donc pas à quoi correspond la mise à disposition de cette personne. Cela implique le renvoi de B. à la voie civile pour cette prétention également (art. 126 al. 2 let. b CPP).

11.2.5 Les prétentions en indemnisation de la société seront traitées ci-dessous, au titre d'indemnité de partie au sens de l'art. 433 CPP.

11.2.6 Partant, la Cour condamne A. à payer à la société B. EUR 574'492.74 et CHF 364'775.42, avec intérêts à 5 % l'an dès le 31 janvier 2017, au titre de remboursement de son dommage.

Elle renvoie B. à agir par la voie civile pour ses autres conclusions civiles (art. 126 al. 2 let. b CPP).

11.3 Des prétentions civiles de C.

11.3.1 La société C. demande que A. soit condamné à lui rembourser le dommage découlant des débits frauduleux opérés par ses comptes par EUR 920'975.- (*recte* : EUR 920'948.-), soit CHF 970'049.- (*recte* : CHF 970'020.-). Elle a en outre requis l'octroi d'une indemnité pour ses frais de représentation en justice par CHF 32'224.35 (cf. ch. B.2.3 *supra*).

La Cour relève qu'une erreur de plume s'est glissée dans la motivation présentée à l'appui des conclusions. En effet, la transaction du 24 mai 2018 porte sur un montant de EUR 389'147.-, et non EUR 389'174.-.

11.3.2 A. est condamné ce jour pour avoir participé au cas concernant la société C. (illicéité de l'acte et faute). Il a pu être établi que, dans ce contexte, c'est un montant total de EUR 994'808.- qui a été détourné (cf. ch. M.2.2 *supra ;* dommage et lien de causalité). Une partie de ces fonds, soit EUR 73'860.-, ont pu être retournés à la société, diminuant d'autant son dommage (id.). Le dommage résiduel de la société C. est ainsi de EUR 920'948.- (EUR 994'808.- - EUR 73'860.-).

11.3.3 Dûment établies, les prétentions de C. en remboursement de son dommage (résiduel) résultant directement des débits frauduleux sont admises et A. est condamné à payer à la société C. la somme de EUR 920'948.- au titre de remboursement de son dommage.

11.3.4 Les prétentions en indemnisation de la société seront traitées ci-dessous, au titre d'indemnité de partie au sens de l'art. 433 CPP.

11.4 Des prétentions des autres parties plaignantes

11.4.1 Hormis C. et B., les autres parties plaignantes n'ont pas chiffré et motivé leurs conclusions civiles, dans le délai que la Cour leur avait imparti par ordonnance du 2 mai 2024 pour ce faire (cf. ch. B.2.3 ss *supra*).

11.4.2 Partant, la Cour renvoie les parties plaignantes G., J., D., E., F., H., I., K., L., M., N., O., P., Q. et R. à agir par la voie civile (art. 126 al. 2 let. b CPP).

11.5 De l'impact de l'issue des actions civiles sur le prononcé d'une créance compensatrice

11.5.1 L'art. 70 a. 1 CP autorise le juge à confisquer des valeurs patrimoniales qui sont le résultat d'une infraction, si elles ne doivent pas être restituées au lésé en rétablissement de ses droits. Lorsque les valeurs patrimoniales à confisquer ne sont plus disponibles, le juge ordonne leur remplacement par une créance compensatrice de l'Etat d'un montant équivalent (art. 71 al. 1 CP *in initio*).

Contrairement à ce qui prévaut sur le plan civil (art. 50 al. 1 CO), la solidarité entre plusieurs prévenus est exclue dans le cas d'une condamnation au paiement d'une créance compensatrice faute de disposition légale en ce sens. Ainsi, la créance compensatrice doit être prononcée à l'encontre de chaque participant en fonction de la part qu'il a reçue. Sur le principe, il est admissible d'allouer au lésé ses conclusions civiles en réparation du dommage subi et de prononcer simultanément une créance compensatrice lorsque le prévenu ne s'est pas encore acquitté des dommages-intérêts dus. Il y a cependant lieu de prévoir un dispositif tendant à éviter que le prévenu ne doive s'acquitter aussi bien de la créance compensatrice que de celle en dommages-intérêts (ATF 150 IV 338 consid. 2.2.1 et références citées).

11.5.2 En l'espèce, A. est condamné ce jour au paiement de dommages-intérêts en mains de B., à hauteur de EUR 574'492.74 et CHF 364'775.42 (auxquels viennent s'ajouter des intérêts à 5 % l'an dès le 31 janvier 2017). Il est également condamné au paiement de dommages-intérêts de EUR 920'948.- en faveur de C. Ainsi, la somme des dommages-intérêts alloués ce jour, soit EUR 1'495'440.74 (EUR 574'492.74 + EUR 920'948.-) et CHF 364'775.42, excède les revenus tirés par A. de son activité criminelle, par EUR 490'468.41 (cf. ch. 4.2.3 *supra*).

Aux débats, le MPC a conclu à ce que le prévenu soit condamné à une créance compensatrice de CHF 500'000.-. Le prononcé d'une créance compensatrice parallèle à l'octroi de dommages-intérêts est certes possible, A. ne s'étant pas, à ce jour, acquitté des prétentions des sociétés lésées. Toutefois, dès lors que la somme des prétentions en dommages-intérêts admises excède celle de l'enrichissement du prévenu, le tribunal ne peut prononcer une créance compensatrice pour la différence entre la première et la deuxième, faute de solidarité entre A. et les autres participants à l'infraction. A. ne disposant d'aucun bien en Suisse et la procédure n'ayant pas permis le prononcé de séquestres susceptibles de faire l'objet d'une exécution forcée d'une créance compensatrice, il ne s'avère pas d'utilité de prononcer une telle créance, équivalente à l'enrichissement de A., en sus de sa condamnation au paiement des dommages-intérêts prononcée ce jour, étant rappelé que la créance compensatrice est en tout état de cause subsidiaire au remboursement du dommage.

Partant, la Cour ne prononce pas de créance compensatrice.

12. Frais de procédure et indemnisation de A.

12.1 <u>De la fixation des frais de procédure</u>

12.1.1 Les frais de procédure, qui se composent des émoluments visant à couvrir les frais et des débours effectivement supportés (art. 422 al. 1 CPP), doivent être fixés conformément au règlement du Tribunal pénal fédéral sur les frais, émoluments, dépens et indemnités de la procédure pénale fédérale (RFPPF; RS 173.713.162), applicable par renvoi de l'art. 424 al. 1 CPP. Les émoluments sont dus pour les opérations accomplies ou ordonnées par la PJF et le MPC dans la procédure préliminaire, ainsi que par la Cour de céans. Les débours sont les montants versés à titre d'avance par la Confédération ; ils comprennent notamment les frais imputables à la défense d'office et à l'assistance judiciaire gratuite, les frais de traduction, les frais d'expertise, les frais de participation d'autres autorités, les frais de port et de téléphone et d'autres frais analogues. Les débours sont fixés au prix facturé à la Confédération ou payé par elle (art. 9 RFPPF). Le montant de l'émolument est calculé en fonction de l'ampleur et de la difficulté de la cause, de la façon de procéder des parties, de leur situation financière et de la charge de travail de chancellerie (art. 5 RFPPF). Les émoluments pour les investigations policières en cas d'ouverture d'une instruction varient entre CHF 200.- et CHF 50'000.- (art. 6 al. 3 let. b RFPPF) ; ceux pour l'instruction terminée par un acte d'accusation peuvent s'étendre à entre CHF 1'000.- et CHF 100'000.- (art. 6 al. 4 let. c RFPPF). Toutefois, le total des émoluments pour toute la procédure préliminaire ne doit pas dépasser CHF 100'000.- (art. 6 al. 5 RFPPF). En ce qui concerne la procédure devant la

Cour de céans, les émoluments devant la Cour composée de trois juges se situent entre CHF 1000.- et CHF 100'000.- (art. 7 let. b RFPPF).

12.1.2 En l'espèce, les débours de la procédure préliminaire se chiffrent à CHF 197'293.20. Un tiers de cette somme, soit CHF 65'764.40, a été mis à la charge de la Confédération par l'ordonnance de classement du 6 mars 2024, qui est entrée en force (MPC 03-01-0007). Dans le présent jugement, la Cour a donc à statuer sur le solde des débours de procédure préliminaire, soit CHF 131'528.80 (2/3 x CHF 197'293.20). Ces débours comprennent des frais qui, en raison de leur nature, ne sont pas susceptibles d'être mis à charge d'un prévenu (frais de détention et de traduction, frais médicaux), pour un total de CHF 84'495.07. Après déduction, dans la proportion définie par l'ordonnance de classement du 6 mars 2024, de la part des débours ne pouvant être imputés au prévenu, soit CHF 56'330.05 (2/3 x CHF 84'495.07), les débours effectifs susceptibles d'être mis à sa charge s'élèvent donc à CHF 75'198.75 (CHF 131'528.80 - CHF 56'330.05).

12.1.3 La cause et les opérations effectuées présentent des difficultés et une ampleur de degré moyen. Partant, la Cour fixe l'émolument de procédure préliminaire à CHF 20'000.- et celui de la procédure de première instance à CHF 15'000.-.

12.1.4 Ainsi, les frais de procédure s'élèvent à CHF 110'198.75 (procédure préliminaire : CHF 20'000.- [émoluments] et CHF 75'198.75 [débours] ; procédure de première instance : CHF 15'000.- [émoluments]).

12.2 <u>De l'imputation des frais de procédure</u>

12.2.1 A teneur de l'art. 426 al. 1 CPP, le prévenu supporte les frais s'il est condamné. Lorsque la procédure fait l'objet d'une ordonnance de classement ou que le prévenu est acquitté, tout ou partie des frais de procédure peuvent être mis à sa charge s'il a, de manière illicite et fautive, provoqué l'ouverture de la procédure ou rendu plus difficile la conduite de celui-ci (art. 426 al. 2 CPP).

12.2.2 A. est condamné pour la très grande majorité des cas pour lesquels il a été mis en accusation (23/25). Les deux cas pour lesquels il est acquitté constituent des tentatives et n'ont engendré, proportionnellement, qu'une part minime des frais de procédure, dont la très grande majorité auraient été encourus même si la procédure n'avait pas porté sur les cas de la société 9 et Q. Du reste, l'ensemble des frais a été engendré par les agissements illicites et fautifs du condamné, qui a provoqué l'ouverture de la procédure par son activité criminelle.

L'ensemble des frais de procédure doivent donc être mis à sa charge, conformément aux prescriptions de l'art. 426 al. 1 et 2 CPP.

12.2.3 Partant, la Cour fixe les frais de la procédure à CHF 110'198.75 (procédure préliminaire : CHF 20'000.- [émoluments] et CHF 75'198.75 [débours] ; procédure de première instance : CHF 15'000.- [émoluments]) et les met intégralement à la charge du prévenu (art. 426 al. 1 et 2 CPP).

12.3 Des prétentions en indemnisation de A.

12.3.1 L'art. 429 al. 1 CPP prévoit que, si le prévenu est acquitté totalement ou en partie ou s'il bénéficie d'une ordonnance de classement, il a droit à une indemnité pour les dépenses occasionnées par l'exercice raisonnable de ses droits de procédure (let. a), son dommage économique (let. b) et à une réparation du tort moral subi en raison d'une atteinte particulièrement grave à sa personnalité, notamment en cas de privation de liberté (let. c). L'autorité pénale examine d'office les prétentions du prévenu mais peut l'enjoindre à les chiffrer et les justifier (art. 429 al. 2 CPP). Toutefois, l'autorité pénale peut réduire ou refuser l'indemnité ou la réparation du tort moral à certaines conditions, en particulier lorsque le prévenu a provoqué illicitement et fautivement l'ouverture de la procédure ou a rendu plus difficile la conduite de celle-ci (art. 430 al. 1 CPP).

12.3.2 A. demande une indemnisation pour ses frais d'avocat, au sens de l'art. 429 al. 1 let. a CPP. Dûment interpellé sur ses éventuelles prétentions (art. 429 al. 2 CPP), il ne fait valoir aucun autre poste d'indemnisation.

Comme exposé ci-avant (cf. ch. 12.2.2 *supra*), A. n'est mis au bénéfice d'un acquittement que pour une part minime des faits qui lui étaient reprochés, sans réelle incidence sur ses frais d'avocat, et il a provoqué illicitement l'ouverture de la procédure. Il n'y a dès lors pas lieu de lui allouer une indemnité au sens de l'art. 429 al. 1 let. a CPP.

13. Indemnités aux parties plaignantes

13.1 Du droit applicable

13.1.1 A teneur de l'art. 433 al. 1 let. a CPP, la partie plaignante peut demander au prévenu une juste indemnité pour les dépenses obligatoires occasionnées par la procédure si elle obtient gain de cause. La partie plaignante adresse ses prétentions à l'autorité pénale ; elle doit les chiffrer et les justifier. Si elle ne s'acquitte pas de cette obligation, l'autorité pénale n'entre pas en matière sur la demande (art. 433 al 2 CPP). L'autorité de fixation procède à une estimation des dépenses nécessaires lorsqu'il n'a pas été possible de chiffrer et prouver précisément celles-ci (WEHRENBERG/FRANK, in Commentaire bâlois du Code de procédure pénale, 3ème éd. 2023, n° 22 ad art. 433 CPP).

13.1.2 La notion de juste indemnité couvre les dépenses et les frais nécessaires pour faire valoir le point de vue de la partie plaignante dans la procédure pénale, ce qui comprend, en premier lieu, les frais d'avocat (ATF 139 IV 102 consid. 4.1 et 4.5; plus récemment, arrêt du Tribunal fédéral 6B_1299/2022 du 12 juillet 2023, consid. 6.1). En application du principe de proportionnalité, les démarches entreprises par l'avocat doivent apparaître nécessaires et adéquates pour la défense du point de vue de la partie plaignante (jugement de la Cour des affaires pénales SK.2024.40 du 31 octobre 2024, consid. 25.1 et références citées).

13.1.3 Les art. 11 ss RFPPF s'appliquent au calcul de l'indemnité de la partie plaignante ayant obtenu gain de cause en tout ou en partie (art. 10 RFPPF; v. aussi art. 73 al. 1 let. c LOAP). Les frais d'avocat comprennent les honoraires et les débours nécessaires, tels que les frais de déplacement, de repas et de nuitée, et les frais de port et de communications téléphoniques (art. 11 al. 1 RFPPF). Les honoraires sont fixés en fonction du temps effectivement consacré à la cause et nécessaire à la défense de la partie représentée. Le tarif horaire est de CHF 200.- au minimum et de CHF 300.- au maximum (art. 12 al. 1 RFPPF). De pratique constante, la Cour des affaires pénales applique un tarif horaire de CHF 230.- (CHF 200.- pour le temps de déplacement et d'attente) aux procédures dont elle connaît lorsque leur degré de difficulté doit être qualifié de moyen, soit lorsqu'elles ne relèvent pas d'une haute complexité et n'exigent pas la maîtrise de plusieurs langues (jugement de la Cour des affaires pénales SK.2023.33 du 27 novembre 2023, consid. 12.1 et références citées).

13.1.4 Ne sont indemnisées que les opérations du mandataire effectuées dans la sauvegarde des droits procéduraux et pour autant qu'elles étaient proportionnées et nécessaires (arrêt du Tribunal fédéral 1B_385/2021 du 25 octobre 2021, consid. 4.2 et références citées). Il y a lieu d'examiner les opérations du mandataire non seulement à la lumière de leur pertinence pour la sauvegarde des droits du mandant, mais aussi au regard de la proportionnalité du temps consacré à cette tâche, par rapport à l'enjeu de la question juridique à résoudre. Le droit à l'indemnisation ne porte pas sur toutes les démarches susceptibles de répondre aux intérêts du mandant mais uniquement sur celles nécessaires à la sauvegarde de ses droits (décisions de la Cour des plaintes BB.2017.125, BB.2017.210 du 15 mars 2018, consid. 7.4). Pour déterminer le temps objectivement nécessaire à la défense d'une cause, le juge fonde son appréciation sur celui qu'y consacrerait un avocat expérimenté, disposant de connaissances approfondies dans le domaine du droit pénal matériel et de la procédure pénale, et qui est donc en mesure de fournir ses prestations de manière ciblée et efficace (arrêt du Tribunal fédéral 6B_888/2021 du 24 novembre 2022, consid. 2.2.1 et références citées).

13.1.5 Seuls les frais effectifs sont au demeurant remboursés au titre des débours (art. 13 al. 1 RFPPF). Les photocopies sont remboursées au prix de 50 centimes pièce et, en cas de grande série, de 20 centimes par photocopie (art. 13 al. 2 let. e RFPPF).

13.1.6 La TVA est de 8 % depuis 2011, de 7,7 % depuis le 1er janvier 2018 et de 8,1 % depuis le 1er janvier 2024 (cf. art. 25 de la loi fédérale du 12 juin 2009 sur la taxe sur la valeur ajoutée [LTVA ; RS 641.20]).

13.2 De l'indemnisation de B.

13.2.1 Me Sébastien Fanti a déposé le 14 mars 2025 sa note d'honoraires pour la défense des intérêts de la société B. (SK 37.851.002 ss). Aux débats, il a conclu à la condamnation de A. au paiement desdits honoraires (cf. ch. C.4 *supra*). Il fait valoir des opérations par CHF 25'156.30, TVA comprise, pour son intervention, à compter de février 2017. La note d'honoraires respecte les principes rappelés ci-avant. En particulier, le nombre d'heures déployées (environ 96 heures) apparaît proportionné aux démarches entreprises. Le taux horaire appliqué, de CHF 230.-, correspond à la pratique de la Cour, à laquelle il n'y a pas lieu de déroger vu l'absence de circonstances exceptionnelles pouvant le justifier.

13.2.2 Ainsi, les opérations présentées par Me Sébastien Fanti constituent des opérations nécessaires à la défense des intérêts de B. qui, de surcroît, a obtenu gain de cause dans la présente procédure, A. étant reconnu coupable d'avoir participé à la fraude dont la société a fait l'objet et les prétentions civiles de B. ayant été très largement admises.

13.2.3 Partant, la Cour condamne A. à verser à B. le montant de CHF 25'156.30 en remboursement de ses dépenses obligatoires occasionnées par la procédure (art. 433 al. 1 let. a CPP).

13.3 De l'indemnisation de C.

13.3.1 Au nom de C., Me Serge Fasel a, par courrier du 29 mai 2024, requis l'octroi d'une indemnité de CHF 32'224.35 pour son intervention et produit une note d'honoraires (SK 37.552.0001 ss). Les opérations y figurant sont comptabilisées à un taux horaire de CHF 400.-, ce qui excède le taux horaire maximal (art. 12 al. 1 RFPPF). Faute de circonstances exceptionnelles, c'est le taux horaire habituel qui doit être retenu, soit CHF 230.-, ce qui réduit le montant total de la note d'honoraire à CHF 18'147.16, TVA comprise. Pour le surplus, la note d'honoraires présentée par Me Serge Fasel respecte les principes rappelés ci-avant. Partant, le montant de CHF 18'147.16 peut être retenu au titre des dépenses nécessaires.

13.3.2 Ainsi, le montant de CHF 18'147.16 peut être retenu au titre des dépenses nécessaires de C. qui, de surcroît, a obtenu gain de cause dans la présente procédure, A. étant reconnu coupable d'avoir participé à la fraude dont la société a fait l'objet et les prétentions civiles de C. ayant été admises.

13.3.3 Partant, la Cour condamne A. à verser à C. le montant de CHF 18'147.16 en remboursement de ses dépenses obligatoires occasionnées par la procédure (art. 433 al. 1 let. a CPP).

13.4 <u>De l'indemnisation de G.</u>

13.4.1 Le 28 mai 2024, Me Christophe Kalbermatten a requis au nom de G. l'octroi d'une indemnité de CHF 13'881.20 pour ses frais d'avocat (SK 37.557.001 s.). A l'appui de la requête, Me Christophe Kalbermatten allègue une trentaine d'heures de travail au taux horaire de CHF 400.-.

13.4.2 Me Christophe Kalbermatten œuvre à la défense des intérêts de la société G. depuis le 20 janvier 2017 (MPC 05-12-0066). Le nombre d'heures de travail invoquées (30 heures) apparaît proportionné à la difficulté de la cause et les enjeux pour la société G. Faute de circonstances exceptionnelles, c'est le taux horaire habituel de CHF 230.- qui doit être retenu pour chiffrer le montant des opérations nécessaires, qui s'élève dès lors à CHF 6'900.-. S'y ajoute la TVA de 7,7%, pour une activité déployée pour l'essentiel avant 2024. Les dépenses nécessaires de G., qui a obtenu gain de cause, peuvent dès lors être estimées CHF 7'500.-, TVA comprise.

13.4.3 Partant, la Cour condamne A. à verser à G. le montant de CHF 7'500.- en remboursement de ses dépenses obligatoires occasionnées par la procédure (art. 433 al. 1 let. a CPP).

Par ces motifs, la Cour prononce :

I. Infractions, peine et expulsion

1. A. est acquitté des chefs d'accusation de soustraction de données (art. 143 CP), d'accès indu à un système informatique (art. 143bis CP) et d'utilisation frauduleuse d'un ordinateur (art. 147 CP) pour les faits décrits aux chiffres 1.3.24 et 1.3.25 de l'acte d'accusation.

2. A. est reconnu coupable d'utilisation frauduleuse d'un ordinateur par métier (art. 147 al. 1 et 2 CP) pour les faits décrits aux chiffres 1.3.1 à 1.3.23 de l'acte d'accusation.

3. A. est condamné à une peine privative de liberté de 48 mois, sous déduction de la détention avant jugement subie, soit 318 jours.

4. A. est expulsé du territoire suisse pour une durée de 5 ans.

5. Les autorités du canton de Vaud sont compétentes pour l'exécution de la peine privative de liberté et de l'expulsion.

6. Les sûretés de CHF 250'000.- (état au 31.12.2024: CHF 252'966.05) déposées sur le compte du Ministère public de la Confédération auprès du Département fédéral des finances, selon la décision du 12 décembre 2022 du Tribunal des mesures de contrainte du canton de Vaud (réf. PC22.022533-CPB), sont maintenues pour garantir l'exécution de la peine privative de liberté prononcée au chiffre I.3 du dispositif du jugement.

II. Parties plaignantes

1. A. est condamné à payer les sommes suivantes à titre de dédommagement:

1.1. B.: EUR 574'492.74 et CHF 364'775.42, avec intérêts à 5 % l'an dès le 31 janvier 2017, B. étant renvoyée à agir par la voie civile pour ses autres conclusions civiles (art. 126 al. 2 let. b CPP) ;

1.2. C.: EUR 920'948.-.

2. Les parties plaignantes G., J., D., E., F., H., I., K., L., M., N., O., P., Q. et R. sont renvoyées à agir par la voie civile (art. 126 al. 2 let. b CPP).

III. Frais de procédure

1. Les frais de la procédure se chiffrent à CHF 110'198.75 (procédure préliminaire: CHF 20'000.- [émoluments] et CHF 75'198.75 [débours]; procédure de première instance: CHF 15'000.- [émoluments]).

2. Les frais de procédure sont intégralement mis à la charge de A. (art. 426 al. 1 et 2 CPP).

3. Aucune indemnité n'est octroyée à A. pour ses frais d'intervention en justice (art. 429 al. 1 let. a CPP).

IV. Indemnités aux parties plaignantes (art. 433 CPP)

A. versera les indemnités suivantes au titre des dépenses obligatoires occasionnées par la procédure (art. 433 al. 1 let. a CPP) :

1. B.: CHF 25'156.30.

2. C.: CHF 18'147.16.

3. G.: CHF 7'500.-.

Au nom de la Cour des affaires pénales
du Tribunal pénal fédéral

Le président La greffière

Distribution (acte judiciaire):
- Ministère public de la Confédération, M. Yves Nicolet, Procureur fédéral, et M. Jean-Philippe Peissard
- Maître Marc Bonnant (pour A.)
- Maître Sébastien Fanti (pour B.)
- Maître Serge Fasel (pour C.)

Distribution (recommandé):
- Aux autres parties plaignantes (version abrégée uniquement, art. 84 al. 4 *in fine* CPP)

Une copie du présent jugement est communiquée à (recommandé):
- Office d'exécution des peines du canton de Vaud (**pour information**)
- Service de la population du canton de Vaud (**pour information**)

L'entrée en force du jugement sera communiquée à:
- Ministère public de la Confédération, Exécution des jugements (en tant qu'autorité d'exécution)
- Office d'exécution des peines du canton de Vaud
- Service de la population du canton de Vaud

Indication des voies de droit

Appel à la Cour d'appel du Tribunal pénal fédéral

L'appel est recevable contre les jugements de la Cour des affaires pénales du Tribunal pénal fédéral qui ont clos tout ou partie de la procédure, contre les décisions judiciaires ultérieures indépendantes et contre les décisions de confiscation indépendantes. L'appel doit être annoncé par écrit ou oralement à la Cour des affaires pénales du Tribunal pénal fédéral **dans le délai de 10 jours** à compter de la communication du jugement (art. 399 al. 1 en lien avec l'art. 398 al. 1 CPP; art. 38a LOAP).

La juridiction d'appel jouit d'un plein pouvoir d'examen sur tous les points attaqués du jugement. L'appel 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, pour constatation incomplète ou erronée des faits ainsi que pour inopportunité (art. 398 al. 2 et 3 CPP).

Si un appel ne porte que sur les conclusions civiles, la juridiction d'appel n'examine le jugement de première instance que dans la mesure où le droit de procédure civile applicable au for autoriserait l'appel (art. 398 al. 5 CPP).

La partie qui annonce l'appel adresse à la Cour d'appel du Tribunal pénal fédéral une déclaration d'appel écrite **dans les 20 jours** à compter de la notification du jugement motivé. Dans sa déclaration, elle doit indiquer si elle entend attaquer le jugement dans son ensemble ou seulement sur certaines parties, les modifications du jugement de première instance qu'elle demande et ses réquisitions de preuves. Quiconque attaque seulement certaines parties jugement est tenu d'indiquer dans la déclaration d'appel, de manière définitive, sur quelles parties porte l'appel (art. 399 al. 3 et 4 CPP).

Observation des délais

Les écrits doivent être remis au plus tard le dernier jour du délai à l'autorité pénale, à la Poste suisse, à une représentation consulaire ou diplomatique suisse ou, s'agissant de personnes détenues, à la direction de l'établissement carcéral (art. 91 al. 2 CPP).

Expédition : 23 octobre 2025