REPUBLIQUE ET CANTON DE GENEVE

POST TENEBRAS LUX

POUVOIR JUDICIAIRE

P/12374/2018 **ACPR/680/2021**

COUR DE JUSTICE

Chambre pénale de recours

Arrêt du mercredi 13 octobre 2021

Entre

A_____, domicilié _____ [VD], comparant par M^e^ Stefan DISCH, avocat, chemin des Trois Rois 2, case postale 5843, 1002 Lausanne,

recourant,

contre l'ordonnance de classement rendue le 12 avril 2021 par le Ministère public,

et

LE MINISTÈRE PUBLIC de la République et canton de Genève, route de Chancy 6B, 1213 Petit-Lancy, case postale 3565, 1211 Genève 3,

intimé.

EN FAIT :

A. **a.** Par acte expédié au greffe de la Chambre de céans le 26 avril 2021, A_____ recourt contre l'ordonnance du 12 avril 2021, notifiée le 14 avril 2021, par laquelle le Ministère public a prononcé le classement de sa plainte.

Le recourant conclut, sous suite de frais et dépens, à l'annulation de l'ordonnance querellée et au renvoi de la procédure au Ministère public pour qu'il "*rende une ordonnance pénale ou un acte d'accusation*".

b. Le recourant a versé les sûretés en CHF 1'000.- qui lui étaient réclamées par la Direction de la procédure.

B. Les faits pertinents suivants ressortent du dossier :

a. Le _____ 2007, A_____ et B_____ ont constitué la société C_____ SA, active dans le commerce de spiritueux. A_____ est également administrateur de la société D_____ SA depuis sa création le _____ 2011.

b. Le 18 octobre 2011, un "*Service Agreement*" a été conclu par C_____ SA, une société sœur française, et B_____ avec A_____ pour confier à ce dernier la gestion opérationnelle des sociétés précitées pour une période de cinq ans.

c. Le 5 octobre 2016, le contrat de A_____ a été résilié avec effet immédiat.

d.a. Le 28 novembre 2016, C_____ SA a déposé plainte pénale contre A_____ auprès du Ministère public de l'arrondissement de E_____ [VD], enregistrée sous le numéro de procédure 1_____, pour des prélèvements injustifiés et des transactions insolites totalisant EUR 8'743'129.-.

d.b. Entendu le 10 janvier 2017 par la police en qualité de prévenu, A_____ s'est vu soumettre un courriel daté du 20 novembre 2014, portant pour objet "*question subtile et confidentielle*", qu'il avait envoyé depuis la boîte "*A_____@C_____.com*" à F_____, auditeur de C_____ SA. Il y expliquait vouloir que sa société "*D_____*" acquière à "*vil prix*" son véhicule de fonction, à savoir une G_____ [marque]. Il a déclaré ne pas se souvenir de ce mail.

e.a. Le 4 avril 2017, C_____ SA, par le biais de son conseil, a versé à la procédure 1_____ un courriel daté du 20 mars 2012, envoyé par F_____ à A_____.

e.b. Le 29 juin 2017, A_____ a déposé plainte pénale contre inconnu pour accès indu à un système informatique auprès du Ministère public de l'arrondissement de E_____ [VD]. La cause a été enregistrée sous le numéro 2_____.

Selon cette plainte, il bénéficiait depuis la création de C_____ SA de l'adresse de messagerie électronique "*A_____@C_____.com*" qu'il utilisait à des fins privées comme professionnelles. Cette adresse était protégée par un mot de passe connu de lui seul et personne n'était autorisé à l'utiliser. Le courriel daté du 20 mars 2012 produit par C_____ SA dans la procédure 1_____, avait trait à sa planification patrimoniale personnelle et relevait du domaine privé. Il n'avait donc pu être obtenu que par le biais d'un accès indu à cette messagerie, ordonné par les "*dirigeants ou propriétaires* […] *de C_____ SA probablement*".

f. Selon le rapport de la police du 20 octobre 2017, la liste des connexions à l'adresse de messagerie "*A_____@C_____.com*" ne permettait pas de retrouver la trace d'un accès indu à ladite boîte.

g. Par lettre du 5 mars 2018, en réponse à une demande du Ministère public vaudois dans la procédure 1_____, C_____ SA a expliqué la manière dont elle avait obtenu le courriel du 20 mars 2012.

À la suite de la résiliation immédiate de son contrat, A_____ avait refusé de lui fournir les livres de comptes en sa possession. Il avait uniquement remis une clé USB contenant un certain nombre de documents. Le conseil d'administration avait alors dû se résoudre à prendre contact avec l'hébergeur du site pour demander le blocage et la reconfiguration de la messagerie "*A_____@C_____.com*", A_____ continuant de l'utiliser après la fin des rapports contractuels. L'accès et la consultation du contenu de cette boîte s'imposaient aussi pour faire la lumière sur les prélèvements litigieux en vue de déposer plainte et pour assurer la poursuite des activités. La prise de connaissance du contenu de cette boîte professionnelle avait permis de mieux cerner le mécanisme des malversations et d'en découvrir d'autres, comme par exemple "*la vente à vil prix de la G_____ à D_____ SA*". La boîte de messagerie était un support de données professionnelles qui lui appartenait. L'accès à ces données respectait les conditions énoncées par le Préposé fédéral à la protection des données et à la transparence (ci-après: PFPDT) concernant le droit de l'employeur de consulter les supports de données privées d'un employé lors de soupçons d'une infraction.

Il ressort des pièces produites par C_____ SA à l'appui de sa lettre les éléments suivants:

- Entre 2016 et 2018, C_____ a cherché à obtenir de A_____ l'ensemble des livres de la société au format papier, tandis que ce dernier affirmait ne pas posséder ces documents et que tout avait été remis avec la clé USB.

- Dans le cadre d'une procédure pénale liechtensteinoise ouverte contre A_____, le Tribunal princier a reconnu à C_____ SA, partie plaignante, un intérêt légitime à accéder au dossier, compte tenu des soupçons suffisants de détournements de ses actifs.

h. Par lettre de son conseil du 28 mars 2018, A_____ a relevé que C_____ SA avait expressément reconnu, dans sa lettre du 5 mars 2018, avoir "*craqué*" sa messagerie électronique alors que les actes reprochés, outre qu'ils étaient contestés, ne justifiaient pas une telle démarche.

i. Le 26 avril 2018, à la suite d'un ordre de dépôt du Ministère public vaudois, la société H_____ SA, sise à Genève, en charge de l'informatique de C_____ SA, a indiqué avoir reçu, au mois d'octobre 2016, une demande pour changer le mot de passe de A_____ après le départ de ce dernier. La boîte "*A_____@C_____.com*" recevait également les messages envoyés sur les adresses génériques de la société, raison pour laquelle il avait été demandé d'y accéder. Le contenu récupéré s'était révélé quasiment vide et une restauration à une date antérieure avait été effectuée.

j. Le 1er mai 2018, C_____ SA a complété ses explications.

À la suite d'une séance du conseil d'administration du 7 octobre 2016, B_____ avait prié un tiers, en la personne de I_____, de remplacer A_____ comme personne de contact auprès de l'hébergeur du site internet et des boîtes électroniques qui y étaient liées. I_____ avait obtenu au début du mois de novembre 2016, par le biais de H_____ SA, la reconfiguration de l'adresse "*A_____@C_____.com*" avec un nouveau mot de passe pour y accéder, ce qui avait permis d'en consulter des extraits pour les besoins exposés dans la lettre du 5 mars 2018.

k. Par lettre du 5 juin 2018, I_____ a expliqué être un expert financier et informatique. Il avait été contacté par C_____ SA aux alentours du 10 octobre 2016 pour agir en tant que gérant du site internet de la société et pour les adresses électroniques y relatives. Il avait recommandé et obtenu la reconfiguration de la boîte "*A_____@C_____.com*", comme cela se faisait usuellement dans cette situation.

l. Par ordonnance d'acceptation du for du 16 juillet 2018, le Ministère public de Genève a repris la procédure 2_____ (devenue P/12374/2018) au motif que les serveurs informatiques hébergeant la messagerie électronique étaient situés à K_____ [GE].

m. Le 10 décembre 2018, la Chambre des recours pénale du Tribunal cantonal vaudois a ordonné, dans le cadre de la procédure 1_____, la perquisition des boîtes "*A_____@D_____.ch*" et "*A_____@bluewin.ch*" pour la période allant du 1er janvier 2011 au jour du prononcé de la décision. En substance, la Chambre vaudoise a retenu que des soupçons suffisants existaient quant à l'intention de A_____ de détruire les documents papiers relatifs aux transferts dénoncés, celui-ci ayant déclaré lors d'une audition les avoir entièrement détruits. Il se justifiait donc de disposer au moins de la retranscription des courriels sous ces deux adresses électroniques.

n. Entendu le 4 mars 2019 par le Ministère public zougois sur demande d'entraide, J_____ a déclaré qu'avant de devenir directeur de C_____ SA, il avait reçu le mandat de contrôler ses livres au mois de septembre 2016. À cette occasion, il avait découvert des virements de plus de EUR 8'800'000.- en faveur de comptes privés ou de sociétés dont A_____ était l'ayant droit économique. Le motif indiqué pour ces versements, à savoir "*remboursement prêt actionnaire*", ne correspondait à aucune réalité, A_____ n'ayant jamais investi dans C_____ SA. Les archives que A_____ avait remises à la société après son départ étaient incomplètes et ne contenaient aucun document susceptible d'étayer son droit à ses remboursements. Pour ces raisons, le conseil d'administration avait décidé de réinitialiser l'adresse électronique de A_____ et de suspendre son accès, notamment parce que celui-ci avait continué à l'utiliser après la fin de son contrat.

C. Dans l'ordonnance querellée, le Ministère public, admettant la réalisation d'un accès indu à un système informatique, retient d'abord que la plainte pénale du 29 juin 2017 était tardive. Lors de son audition du 10 janvier 2017, A_____ avait été confronté à un courriel provenant de sa messagerie électronique envoyé à F_____, de sorte qu'il devait savoir, dès cette date, que des tiers avaient pu accéder à ce compte de messagerie.

Ensuite, le Ministère public relève que A_____ était soupçonné, en qualité d'administrateur de C_____ SA, d'avoir ordonné des transferts de fonds sans cause, en sa faveur ou en faveur de sociétés dont il était l'ayant droit économique, pour un montant de plus de EUR 8'000'000.- au préjudice de la société. Les représentants de C_____ SA s'étaient donc inspirés des recommandations du PFPDT pour décider d'accéder à la boîte de messagerie de A_____ compte tenu des soupçons qui pesaient sur lui. La Chambre des recours pénale vaudoise avait même considéré comme justifié de disposer au moins de la transcription des courriels de A_____ sous ses deux adresses électroniques finissant respectivement par "*@D_____.ch*" et *"@bluewin.ch*" au vu du risque de disparition des documents papiers relatifs aux transferts de fonds dénoncés. C_____ SA avait ainsi réagi face à un danger important et à ce point imminent qu'il commandait d'accéder là où elle n'avait pas le droit, à savoir les comptes de messagerie de A_____, pour sauvegarder ses intérêts légitimes. Certes, C_____ SA, soit pour elle ses représentants, auraient dû utiliser une voie légale afin de parvenir au même but mais elle pensait se trouver dans un état

de nécessité putatif justifiant ses agissements. Pour toutes ces raisons, le classement de la procédure s'imposait.

D. **a.** Dans son recours, A_____ soutient que sa plainte n'était pas tardive. Le courriel qui lui avait été soumis lors de son audition du 10 janvier 2017 ne lui permettait pas de considérer qu'il avait été victime d'une extraction de ses données. C_____ SA avait montré une détermination à agir en marge de la loi puisqu'elle avait agi alors que les transferts dénoncés étaient reconnus, documentés et chiffrés. Les organes de C_____ SA n'avaient en outre jamais invoqué les recommandations du PFPDT. L'arrêt du Tribunal cantonal vaudois ne concernait pas l'adresse de messagerie "*A_____@C_____.com*" et recommandait la voie légale, ce qui n'avait pas été respecté par les représentants de C_____ SA. Il n'y avait pas de danger important et imminent puisque: la société disposait d'une copie complète de la boîte de messagerie en cause, la voie légale était ouverte et les documents papier concernant les transferts de fonds n'avaient jamais disparu mais se trouvaient auprès de la banque et du réviseur. L'état de nécessité putatif devait également être nié du fait qu'aucun danger imminent n'existait et que les représentants de la société étaient suffisamment aguerris au monde des affaires pour ne pas se méprendre sur la situation juridique et l'urgence d'agir par une voie paralégale.

b. À réception des sûretés, la cause a été gardée à juger sans échange d'écritures ni débats.

EN DROIT :

1. Le recours est recevable pour avoir été déposé selon la forme et dans le délai prescrits (art. 385 al. 1 et 396 al. 1 CPP), concerner une ordonnance sujette à recours auprès de la Chambre de céans (art. 393 al. 1 let. a CPP) et émaner du plaignant qui, partie à la procédure (art. 104 al. 1 let. b CPP), a qualité pour agir, ayant un intérêt juridiquement protégé à la modification ou à l'annulation de la décision querellée (art. 382 al. 1 CPP).

2. La Chambre pénale de recours peut décider d'emblée de traiter sans échange d'écritures ni débats les recours manifestement mal fondés (art. 390 al. 2 et 5 *a contrario* CPP). Tel est le cas en l'occurrence, au vu des considérations qui suivent.

3. L'art. 319 al. 1 CPP prévoit divers motifs de classement de la procédure par le Ministère public. Tel doit notamment être le cas lorsque les éléments constitutifs d'une infraction ne sont pas réunis (let. b), lorsqu'il est établi que certaines conditions à l'ouverture de l'action pénale ne peuvent pas être remplies ou que des empêchements de procéder sont apparus (let. d) ou lorsque des dispositions légales permettent de renoncer à toute poursuite ou à toute sanction (let. e).

La décision de classer la procédure doit être prise en application du principe "*in dubio pro duriore*". Celui-ci signifie qu'en règle générale, un classement ou une non-entrée en matière ne peut être prononcé par le ministère public que lorsqu'il apparaît clairement que les faits ne sont pas punissables ou que les conditions à la poursuite pénale ne sont pas remplies. Le ministère public dispose, dans ce cadre, d'un pouvoir d'appréciation. La procédure doit se poursuivre lorsqu'une condamnation apparaît plus vraisemblable qu'un acquittement ou lorsque les probabilités d'acquittement et de condamnation apparaissent équivalentes, en particulier en présence d'une infraction grave. En effet, en cas de doute s'agissant de la situation factuelle ou juridique, ce n'est pas à l'autorité d'instruction ou d'accusation mais au juge matériellement compétent qu'il appartient de se prononcer (ATF 143 IV 241 consid.2.2.1 p. 243 ; 138 IV 86 consid. 4.1.2 p. 91).

4. **4.1.** Selon l'art. 143bis CP, quiconque s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

4.1.1. Pour que l'infraction soit réalisée, il faut être en présence de trois conditions, soit un accès à un système informatique, appartenant à autrui et spécialement protégé, qui soit indu et intentionnel (S. METILLE / J. AESCHLIMANN, *Infrastructures et données informatiques : quelle protection au regard du code pénal suisse ?*, *in* Revue pénale suisse 2014, vol. 132, p. 283/297). Pour être considéré comme indu, l'accès doit avoir été effectué sans droit, c'est-à-dire qu'il n'a pas été autorisé par la loi, par le consentement de la victime ou par un autre motif justificatif (S. METILLE / J. AESCHLIMANN, *op. cit*., p. 301).

4.1.2. En matière de traitement de données personnelles, l'art. 328*b* CO stipule que l'employeur ne peut traiter des données concernant le travailleur que dans la mesure où ces données portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail. En outre, les dispositions de la loi fédérale du 19 juin 1992 sur la protection des données sont applicables.

Le PFPDT a publié plusieurs documents, en particulier un guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail à l'attention de l'économie privée (cf. le site Internet www.leprepose.ch).

Il ressort notamment de ce guide que l'employeur, par le droit dont il dispose de réglementer la conduite des travailleurs dans son exploitation, peut réglementer la navigation sur Internet et l'utilisation du courrier électronique. Avant de pouvoir installer une surveillance, l'employeur doit informer préalablement son personnel et élaborer un règlement relatif à celle-ci, *i.e.* ses conditions. À noter toutefois que

lorsque l'employeur soupçonne de manière fondée un employé d'avoir commis ou de s'apprêter à commettre une infraction pénale, l'employeur pourra se fonder sur un intérêt prépondérant privé pour ne pas informer préalablement la personne mise en cause des mesures de surveillance qu'il entend prendre à son égard pour pouvoir, par exemple, sauvegarder des preuves (S. METILLE, *La surveillance électronique des employés*, *in* Internet au travail, 2014, p. 116; cf. guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail, annexe B: règlement-type).

Le Tribunal fédéral s'est référé aux modalités préconisées par le PFPDT en matière de surveillance pour délimiter ce qui est admissible de ce qui est excessif, donnant de fait une force particulière à ces recommandations (ATF 139 II 7 = JT 2013 II 187, 188; S. METILLE, *op. cit.*, p. 104; R. WYLER / B. HEINZER, *Droit du travail*, Berne 2019, p. 423).

4.2. Le droit de porter plainte se prescrit par trois mois (art. 31, 1ère phrase, CP). Ce délai court du jour où l'ayant droit a connu l'auteur de l'infraction (art. 31, 2ème phrase, CP) ainsi que l'acte délictueux, ce qui, selon la jurisprudence, implique de savoir de manière sûre et fiable que les éléments constitutifs d'une infraction sont donnés, de sorte qu'une procédure dirigée contre l'auteur aurait de bonnes chances d'aboutir (ATF 126 IV 131 consid. 2a; arrêt du Tribunal fédéral 6B_1113/2014 du 28 octobre 2015, consid. 2.1).

L'observation du délai de plainte fixé à l'art. 31 CP est une condition d'exercice de l'action publique, qui justifie un refus de mettre en œuvre la poursuite pénale lorsqu'elle n'est pas réalisée, ou le prononcé d'un classement lorsque le juge d'instruction a procédé à des mesures d'instruction (A. KUHN / Y. JEANNERET (éds), *Commentaire romand : Code de procédure pénale suisse*, Bâle 2011, n. 10 ad art. 319;G. PIQUEREZ / A. MACALUSO, *Procédure pénale suisse*, 3ème éd., 2011, p. 537 n. 1553 et 1555).

4.3. En l'espèce, le recourant a déposé plainte le 29 juin 2017 après sa découverte, dans la procédure 1_____, du courriel daté du 20 mars 2012 reçu du réviseur de la société. On comprend de sa plainte que ses soupçons d'un accès indu à sa messagerie électronique par des "*dirigeants ou propriétaires* […] *de C_____ SA*" sont nés du fait que ledit mail avait trait à la planification de son patrimoine personnel, sujet qui relevait du domaine privé.

Auparavant, lors de son audition du 10 janvier 2017, le recourant avait été invité à se déterminer sur un courriel du 20 novembre 2014 qu'il avait écrit à ce même réviseur. Dans ce courriel – désigné comme "*confidentiel*" dans son objet – il formulait le souhait que la société dont il était administrateur acquière "*à vil prix*" son véhicule de fonction, de marque G_____. De par sa nature incriminante, ce courriel devait être

dissimulé à la société. Ce n'est d'ailleurs pas un hasard s'il a servi par la suite à étayer la plainte contre le recourant déposée par la société par-devant le Ministère public vaudois. Ainsi, le plaignant n'a manifestement pas remis ce courriel à la société, ni ne l'a rendu accessible d'une quelconque manière. Partant, il devait déduire, lorsqu'il en a pris connaissance durant son audition, que son obtention ne pouvait découler que d'un accès à sa messagerie, à l'instar de ce qu'il a compris être le cas pour le courriel du 20 mars 2012.

Les arguments du recourant pour démentir ce constat tombent à faux. D'abord, il relève que lors de son audition, un seul courriel lui avait été présenté. Or, il ressort de sa plainte que celle-ci est consécutive à la production d'un unique courriel également. Ensuite, les deux courriels litigieux concernent des échanges entre lui et le réviseur de la société. Enfin, rien ne lui permettait d'attribuer une provenance litigieuse à l'un des courriels et pas à l'autre. Dans sa plainte, le recourant déduit de sa prise de connaissance du courriel du 20 mars 2012 que celui-ci n'avait pu être obtenu que par un accès indu à sa messagerie. Partant, il faut en conclure que l'origine du courriel n'était pas spécifiée lors de sa production par la société, mais la situation n'était pas différente pour le courriel soumis au recourant lors de son audition. De surcroît, on peine à imaginer quel changement de circonstances entre la prise de connaissance des deux mails, intervenue dans un intervalle de trois mois au maximum, justifierait une interprétation différente de leur provenance.

En résumé, si le recourant a pu soupçonner la commission d'un accès indu à sa messagerie avec sa prise de connaissance du courriel du 20 mars 2012, il y a lieu de considérer qu'il devait aboutir au même résultat lorsqu'il s'est vu soumettre, lors de son audition du 10 janvier 2017, le mail du 20 novembre 2014. En conséquence, la plainte aurait dû être déposée le 10 avril 2017 au plus tard.

Déposée le 29 juin 2017, sa plainte pour accès indu à un système informatique est ainsi tardive. La décision de classement est donc justifiée pour ce motif.

4.4. En tout état, l'accès à la boîte électronique n'était pas indu au sens de l'art. 143bis CP, étant relevé que l'autorité de recours possède un plein pouvoir d'examen en droit et n’est pas liée par la motivation de l'autorité précédente dont elle a à connaître des décisions (art. 6 et 7 CPP, arrêt du Tribunal fédéral 5A_795/2009 du 10 mars 2010 consid. 3.1, non publié aux ATF 136 III 123; ATF 126 I 97 consid. 2b p. 102 s.).

Le conseil d'administration de la société a décidé au mois d'octobre 2016 d'accéder à la messagerie électronique du recourant, prenant appui sur les recommandations du PFPDT comme elle l'explique dans sa lettre du 5 mars 2018, alors qu'elle le soupçonnait déjà d'avoir commis des infractions à son détriment. Ces soupçons sont en effet nés avec le contrôle comptable effectué au mois de septembre 2016, qui avait

fait la lumière sur des versements de plus de EUR 8'000'000.- en faveur de comptes privés ou de sociétés dont le plaignant était l'ayant droit économique. L'accès à la messagerie avait donc pour but de confirmer ces suspicions et, cas échéant, de les documenter.

Dans ce contexte, il faut admettre à la société, soit pour elle ses représentants, un intérêt prépondérant à la consultation de cette boîte électronique. La gravité des actes reprochés au recourant, soit le détournement de plus de EUR 8'000'000.-, et l'incertitude quant au sort des documents papiers relatifs à ces transferts de fonds, contrebalançaient le droit au recourant au respect de sa sphère privée sur sa messagerie professionnelle.

Il sied de constater que le bien-fondé des soupçons a été reconnu par le Tribunal princier du Liechtenstein, tandis que les intérêts de la société à accéder aux boîtes de messagerie privées du recourant ont été confirmés par le Tribunal cantonal vaudois.

En application des principes rappelés ci-avant concernant la surveillance des employés, la société était ainsi guidée dans sa démarche par des motifs justifiés, en faveur d'intérêts prépondérants. Par conséquent, la reconfiguration de la messagerie électronique en vue de son accès et de sa consultation n'était pas indue. Dès lors, l'un des éléments constitutifs de l'infraction faisait défaut (M. DUPUIS / L. MOREILLON / C. PIGUET / S. BERGER / M. MAZOU / V. RODIGARI (éds), *Code pénal - Petit commentaire*, 2e éd., Bâle 2017, n. 18 et 19 ad art. 143bis).

Pour cette raison aussi mais principalement au motif que la plainte était tardive, la décision du Ministère public de ne pas entrer en matière ne prête pas le flanc à la critique.

5. Justifiée, l'ordonnance querellée sera donc confirmée.

6. Le recourant, qui succombe, supportera les frais envers l'État, fixés en totalité à CHF 1'000.- (art. 428 al. 1 CPP et 13 al. 1 du Règlement fixant le tarif des frais en matière pénale, RTFMP ; E 4 10.03).

* * * * *

PAR CES MOTIFS,
LA COUR :

Rejette le recours.

Condamne A_____ aux frais de la procédure de recours, arrêtés à CHF 1'000.-.

Dit que ce montant sera prélevé sur les sûretés versées.

Notifie le présent arrêt ce jour, en copie, à A_____, soit pour lui son conseil, et au Ministère public.

Siégeant :

Madame Corinne CHAPPUIS BUGNON, présidente; Monsieur Christian COQUOZ et Madame Daniela CHIABUDINI, juges; Madame Olivia SOBRINO, greffière.

La greffière :	La présidente :
Olivia SOBRINO	Corinne CHAPPUIS BUGNON

Voie de recours :

Le Tribunal fédéral connaît, comme juridiction ordinaire de recours, des recours en matière pénale au sens de l'art. 78 de la loi sur le Tribunal fédéral du 17 juin 2005 (LTF; RS 173.110); la qualité et les autres conditions pour interjeter recours sont déterminées par les art. 78 à 81 et 90 ss LTF. Le recours doit être formé dans les trente jours qui suivent la notification de l'expédition complète de l'arrêt attaqué.

Le recours doit être adressé au Tribunal fédéral, 1000 Lausanne 14. Les mémoires doivent être remis au plus tard le dernier jour du délai, soit au Tribunal fédéral soit, à l'attention de ce dernier, à La Poste Suisse ou à une représentation diplomatique ou consulaire suisse (art. 48 al. 1 LTF).

P/12374/2018 **ÉTAT DE FRAIS**

COUR DE JUSTICE

Selon le règlement du 22 décembre 2010 fixant le tarif des frais en matière pénale (E 4 10.03).

Débours (art. 2)		
- frais postaux	CHF	10.00
Émoluments généraux (art. 4)		
- délivrance de copies (let. a)	CHF	
- délivrance de copies (let. b)	CHF	
- état de frais (let. h)	CHF	75.00
Émoluments de la Chambre pénale de recours (art. 13)		
- décision sur recours (let. c)	CHF	915.00
-	CHF	
Total	CHF	**1'000.00**