Jugt. 2628/2014 **not.3723/12/CD**

Restit.

AUDIENCE PUBLIQUE DU 16 OCTOBRE 2014

Le Tribunal d'arrondissement de et à Luxembourg, chambre correctionnelle, a rendu le jugement qui suit :

Dans la cause du Ministère Public contre

X.)
né le (…) à (…),
demeurant L-(…), (…),

prévenu

FAITS :

Par citation du **3 décembre 2013** le Procureur d'Etat près le Tribunal d'arrondissement de et à Luxembourg a requis le prévenu de comparaître à l'audience publique du **20 mars 2014** devant le Tribunal correctionnel de ce siège pour y entendre statuer sur les préventions suivantes :

vol, vol à l'aide de fausses clés, infractions à l'article 509-1 du Code Pénal ; infraction à l'article 82 de la loi modifiée du 18 avril 2011 sur les droits d'auteur, les droits voisins et les bases de données.

A cette audience, l'affaire fut contradictoirement remise au 24 septembre 2014.

A cette audience, le vice-président constata l'identité du prévenu et lui donna connaissance des actes qui ont saisi le tribunal.

Les témoins **T1.)** et **T2.)** furent entendus, chacun séparément, en leurs déclarations orales après avoir prêté le serment prévu à l'article 155 du Code d'instruction criminelle.

Le prévenu **X.)** fut entendu en ses explications et moyens de défense, lesquels furent plus amplement développés par Maître Nicky STOFFEL, avocat à la Cour, demeurant à Luxembourg.

Le représentant du Ministère Public, Gilles HERRMANN, substitut principal du Procureur d'Etat, résuma l'affaire et fut entendu en ses réquisitions.

Le Tribunal prit l'affaire en délibéré et rendit à l'audience publique de ce jour, date à laquelle le prononcé avait été fixé, le

J U G E M E N T q u i s u i t :

Vu le rapport n° SPJ-41/2012/JDA19858.1 ENPA dressé en date du 3 février 2012 par la Police grand-ducale, Service de Police Judicaire, Section nouvelles technologies.

Vu le rapport n° SPJ-41/2012/JDA19858.10 ENPA dressé en date du 20 mars 2012 par la Police grand-ducale, Service de Police Judicaire, Section nouvelles technologies.

Vu le rapport n° SPJ-41/2012/JDA19858.14 ENPA dressé en date du 6 avril 2012 par la Police grand-ducale, Service de Police Judicaire, Section nouvelles technologies.

Vu le rapport n° SPJ-41/2012/JDA19858.23 ENPA dressé en date du 16 juillet 2012 par la Police grand-ducale, Service de Police Judicaire, Section nouvelles technologies.

Vu le rapport de police n° SPJ-41/2012/JDA19858.30 ENPA dressé en date du 1er octobre 2012 par la Police grand-ducale, Service de Police Judicaire, Section nouvelles technologies.

Vu la citation à prévenu du 10 juillet 2013 régulièrement notifiée à **X.)**

Vu l'ordonnance de renvoi numéro 371/13 de la Chambre du Conseil du 20 février 2013.

Vu l'instruction diligentée par le Juge d'Instruction.

QUANT AUX FAITS

1. Les éléments de l'enquête

Il résulte des éléments du dossier que les données médicales recueillies par le service médico-sportif figurent dans une base de données dénommée « SPMED », gérée par le Centre des technologies de l'information de l'Etat (CTIE) pour compte du département ministériel des sports.

En date du 19 janvier 2012, le fonctionnaire **F.)**, dûment mandaté par le ministre (…), a porté plainte parce qu'un ou plusieurs auteurs avaient obtenu connaissance des données d'accès à la base de données SPMED et y avaient accédé.

Il s'avère que **P.)**, préposé du CERT Gouvernemental avait été informé de l'existence d'une faille de sécurité informatique par **T2.)**, travaillant pour compte du CIRCL (Computer Incident Response Center Luxembourg). Le 10 janvier 2012, à 10.14 heures, **T2.)** avait en effet envoyé, depuis l'adresse « info@circl.lu », un email intitulé « Examen Médico Sportif Portal » dans lequel il avertit quant à l'usage d'un mot de passe facilement prédictible (suite logique des touches d'un clavier) et précise : « *The reporter told us that the credentials were discovered in a public space (Doctors Office)* ».

Les données d'accès utilisées par les auteurs étaient celles attribuées au docteur **D.)**.

Cette dernière explique lors de son audition qu'elle ferait ses consultation médico-sportives en général dans son cabinet à (…). L'Institut National des Sports aurait mis à sa disposition un ordinateur portable, qui servirait uniquement à se connecter à la base de données du service médico-sportif. Le docteur **D.)** admet que les données d'accès étaient notées sur un post-it apposé sur cet ordinateur. Elle suspecte **X.)** d'être l'auteur des accès non autorisés, puisque celui-ci avait demandé un rendez-vous urgent pour renouveler sa licence et qu'il est passé dans son cabinet le 5 janvier 2012. D'après **D.)**, **X.)** était le dernier patient de la journée, et par ailleurs le seul adulte, les autres ayant été des enfants âgés de 10 ans ou moins. L'assistante procéderait aux premières analyses, telle la mesure du poids et le test des yeux et des poumons. Par la suite, **X.)** aurait été seul pendant 5 à 6 minutes dans la salle d'examen, avant qu'elle ne vienne pour l'examen médical.

L'enquête a permis de constater que non seulement les données d'accès avaient été compromises, mais qu'elles ont encore été utilisées pour accéder à la base de données SPMED. Les différents fichiers « log » enregistrant les accès, tentatives d'accès et opérations sur base de données ont été analysés. Sur base des déclarations du docteur **D.)**, les agents ont filtré les données qui ne correspondaient pas à un accès légitime par le médecin.

Il s'est avéré que le premier accès non autorisé avait eu lieu le 5 janvier 2012, à 22.04 heures.

Plusieurs adresses IP ont pu être identifiées, notamment :

- L'adresse 176.(…).76 provenait du fournisseur de services VPN « **(...)** ».

- Les adresses 94. (…).98 et 94. (…).239, provenant du fournisseur d'accès TANGO MOBILE. L'enquête sur les serveurs de l'Etat a permis de constater qu'une de ces adresses IP avait également servi pour se connecter au serveur E-Mail du Service National de la Jeunesse.

Les données recueillies par la police judiciaire ont encore permis de constater qu'en date du 5 janvier 2012, des recherches avaient été effectuées avec les mots-clef « **X.)** », « **A.)** », « **B.)** », « **B'.)** » et « **C.)** ». Les fiches des sportifs **X.)**, **E.)**, **G.)** et **C.)** avaient été consultées.

Une perquisition du 22 février 2012 auprès de l'opérateur TANGO MOBILE a permis d'attribuer plus précisément les adresses IP concernées :

- Les adresses IP 94. (…).98 et 94. (…).239 étaient, au moment des accès en question, attribués à l'abonnement souscrit par la mère de **T2.)**.

- L'adresse IP 94. (…).159 était attribuée à une voisine du docteur **D.)**, dont le réseau WiFi n'était pas sécurisé, de sorte que l'ordinateur portable du SPMED s'y connectait régulièrement.

Une perquisition du 28 février 2012 auprès du Service National de la Jeunesse a permis de constater que la conjonction de l'adresse IP 94. (…).98 avec la date du 6 janvier 2012, 02 :04, correspondait au compte de courrier électronique « **T2.)**@youth.lu », attribué à **T2.)**.

En date du 4 avril 2012, les agents de police ont, sur base d'une ordonnance du juge d'instruction, procédé à une perquisition au domicile privé de **X.)**. Ils y ont saisi notamment deux ordinateurs MacBook, deux téléphones iPhone, un iPad et un disque dur. Lors de sa première audition par la police, **X.)** admet s'être rendu le 5 janvier 2012 au service médico-sportif pour renouveler sa licence de volleyball. Il ne conteste pas qu'il était pendant un certain temps seul dans la salle des examens médicaux et qu'il y avait un ordinateur portable sur lequel était fixé un post-it. Il déclare ne pas souhaiter répondre à la question de savoir s'il a pris ou non une photo de ce post-it. Il refuse également de répondre à la question de savoir s'il a tenté d'accéder à la base de données SPMED.

A la même date du 4 avril 2012, une perquisition eut lieu au domicile privé de **T2.)**. Y ont été saisis un grand nombre d'ordinateurs, de téléphones de disques durs et autres supports informatiques. Ce dernier refusait également de fournir les codes permettant de décrypter les supports informatiques, en expliquant que ceux-ci pouvaient contenir des données sensibles en relation avec son travail pour le CICL. Lors de son audition auprès de la police, **T2.)** explique travailler pour le « Computer Incident Response Center Luxembourg » (CIRCL). Il dit avoir rencontré **X.)** à une fête d'anniversaire qui avait été organisée le 6 janvier 2012. Ce dernier lui aurait

expliqué que lors de son examen au service médico-sportif, il aurait fait une photo intéressante. Il lui aurait montré la photo d'un post-it contenant un identifiant, un code d'accès et un URL. **T2.)** dit avoir noté ces données dans son téléphone portable. Le soir, vers 22.00 heures, il se serait servi de son ordinateur pour accéder à la base de données SPMED ; il admet avoir consulté diverses fiches pour tester dans quelle mesure des informations critiques étaient accessibles.

En date du 27 avril 2012, la police a procédé à une perquisition auprès de la société **SOC1.)** pour récupérer des données.

Dans leur rapport précité du 16 juillet 2012, les agents enquêteurs arrivent aux conclusions suivantes suite à ces perquisitions :

La perquisition auprès de **SOC1.)** a permis de constater que **X.)** payait un abonnement pour un service VPN auprès du fournisseur **(...)**, et ce durant la période des accès litigieux. L'analyse du contenu de son ordinateur portable a confirmé que le logiciel afférent était installé.

Tant l'ordinateur que le téléphone portable de **X.)** étaient cryptographiés et le prévenu refusait de fournir le code. Les services de police ont néanmoins réussi à déterminer le code d'accès de l'ordinateur, et il s'est avéré que ce même code permettait de débloquer également le téléphone portable iPhone.

Sur le téléphone iPhone, les agents ont trouvé deux fichiers image « IMG_0063.jpg » et « IMG_0064.jpg », enregistrés le 5 janvier 2012 à 17.09 heures, et montrant une partie d'un ordinateur portable avec un post-it contenant le nom d'utilisateur **ABC.)**, deux anciens codes d'accès barrés, ainsi qu'un code d'accès non barré.

Sur l'ordinateur de **X.)**, les agents ont pu trouver dans les fichiers log d'un programme de protection contre les logiciels malveillants (*AntiMalware*) une inscription correspondant à un accès en date du 9 janvier 2012, vers 17.01 heures, à la base de données SPMED. D'après les données du CTIE, c'est à ce moment qu'il y avait eu un accès à la fiche de **C.)**.

Dans l'historique du navigateur Internet « Google Chrome », les agents ont également décelé une entrée indiquant que le 5 janvier 2012, à 22.02 heures, une connexion avait été établie vers la page de login de la base de données SPMED.

Les agents ont encore trouvé divers courriers électronique, et notamment :

- Un courrier électronique envoyé le 10 janvier 2012 au vice-président du parti pirate luxembourgeois ; l'annexe intitulée « medicoleaks.zip » contenait

l'électrocardiogramme de **X.)** et 14 captures d'écran (*Screenshot*) de la base de données SPMED.

- Deux courriers électroniques envoyés à des journalistes luxembourgeois et concernant une éventuelle faille dans la sécurité de la base SPMED.

Lors de son audition du 15 mai 2012, le prévenu **X.)** avait réitéré son refus de fournir les codes d'accès ; il expliquait vouloir protéger sa sphère privée et se méfier des autorités de poursuites, ce d'autant plus que l'ordonnance de perquisition serait arrivée aux mains de RTL. Confronté à la photo du post-it avec l'identifiant et le code d'accès, il déclare : « *Ich möchte zu diesem Zeitpunkt keine Aussage hierzu machen* ». Il refuse également de faire des déclarations concernant les accès opérés à travers le service **(...)** en date des 5 et 9 janvier 2012. Il admet uniquement être abonné à ce service, mais cet abonnement serait utilisé par d'autres membres de sa famille et par des collègues.

T2.) avait également refusé de fournir le code d'accès à son ordinateur. Il a uniquement accepté de débloquer lui-même son ordinateur et de permettre aux agents d'effectuer une recherche en sa présence. Dans le logiciel « *EverNote* », ils ont trouvé une notice indiquant qu'il y a eu un accès aux données médicales de **H.)**.

Sur Commission rogatoire internationale, les autorités américaines ont fourni, par courrier du 17 août 2012, les données de connexion provenant de la société **(...)**. Sur cette base, la police a pu constater que l'adresse IP 176. (…).76 était, pendant les périodes d'accès à la base de données SPMED, attribuée à l'utilisateur « **x.)** » qui, d'après les documents de facturation de la société **(...)**, correspond à **X.)**, demeurant à (…), le paiement étant effectué par le service **SOC1.)**.

2. Déclarations auprès du Juge d'Instruction

Lors de son audition auprès du juge d'instruction en date du 26 octobre 2012, **T2.)** explique qu'il a fait la connaissance de **X.)** parce que ce dernier était venu le voir pour lui signaler quelque chose qui pourrait l'intéresser dans sa fonction de CERT national. **X.)** lui aurait montré une photo avec un identifiant et un mot de passe. Il lui aurait dit qu'il était passé au service médico-sportif et que cela pourrait l'intéresser dans le cadre de la protection des données. Il n'aurait pas donné d'autres détails, et **T2.)** admet ne pas en avoir demandés.

T2.) explique s'être connecté à la page en question et avoir ouvert en même temps un « ticket » dans leur système pour pouvoir retracer ce qui se passait. Il admet avoir regardé diverses fiches et avoir constaté que des données hautement sensibles étaient accessibles. Il avait agi dans le cadre de son travail. Le lundi

d'après, il ne se serait pas occupé du dossier, en raison d'un incident important auprès d'un industriel. Le mardi, il aurait envoyé le ticket dans l'affaire du service médico-sportif.

X.) a été inculpé et entendu par le juge d'instruction en date du 26 octobre 2012. Accusé d'avoir volé un identifiant et un mot de passe pour accéder à la base de données du SPMED, il réplique : « Tout d'abord, je voudrais dire que le terme voler est faux. Je ne veux rien dire en ce qui concerne le reste. Je n'arrive plus à reconstituer ces journées totalement dans ma tête et je ne saurai vous dire ce que j'ai fait exactement à telle ou telle date ».

Il admet avoir été au service médico-sportif de (…). Dans la pièce dans laquelle les tests médicaux étaient effectués, il y aurait eu un ordinateur portable avec un post-il. Il admet l'avoir photographié ; il ne veut pas se prononcer quant à l'utilisation qu'il a faite de ces informations.

Confronté au fait que les fiches consultées concernent des personnes de son entourage, et qu'il s'agit d'un indice à sa charge, **X.)** réplique qu'il s'agit simplement d'un indice. Il admet payer un abonnement auprès de **(...)**, mais 10 à 12 personnes de son entourage y auraient accès. Il aurait un « entourage qui s'intéresse à des failles de sécurité ».

Il estime scandaleux que les données d'accès soient accessibles aussi facilement ; cela le révolterait.

L'inculpé n'a pas souhaité se prononcer sur la plupart des questions que le juge d'instruction lui a posées par la suite. Il voudrait bien se souvenir, mais ce serait compliqué de retracer des dates précises.

3. Déclarations à l'audience

A l'audience, le témoin **T1.)** confirme le déroulement de l'enquête. Il rappelle qu'il a pu être constaté que le 5 janvier 2012, vers 22h04, la base de données SPMED-DB a été accédée via une connexion anonymisée dite VPN.

L'avocat de la défense s'interroge si **X.)** était le seul à pouvoir accéder via la connexion VPN. Le témoin explique que normalement, plusieurs personnes se partagent dans les réseaux VPN une même adresse-IP. Normalement, une seule personne pourrait cependant utiliser la connexion VPN au même moment.

Sur question de la défense, le témoin explique qu'il ne résulte pas des éléments recueillis lors de l'enquête pendant combien de temps l'accès à la base de données SPMED a été maintenue. Il estime que pour réaliser les différentes recherches et les *Screenshot*, quelques minutes seraient nécessaires.

Le témoin **T2.)** témoigne à l'audience qu'il y a deux ans, il avait rencontré **X.)** à une fête d'anniversaire d'une connaissance commune. **X.)** lui aurait montré une photo montrant un post-it contenant un mot de passe. Il lui aurait dit qu'il s'agissait d'un mot de passe pour accéder à la base de données du service médico-sportif. Il aurait noté le mot de passe et, dès qu'il était rentré à la maison, il aurait vérifié si la faille informatique alléguée existait vraiment. Il explique avoir agi dans le cadre de son activité professionnelle au sein du CIRCL (Computer Incident Response Center Luxembourg). La mission de cette autorité consisterait spécifiquement à recueillir des déclarations, parfois anonymes, quant à des failles informatiques, et à intervenir auprès des opérateurs responsables pour qu'il y soit remédié. Constatant que l'accès était réellement possible et que le mot de passe était donc compromis, il aurait ouvert un « ticket » dans leur système, de sorte que le dossier aurait suivi son chemin.

Sur question de la défense, **T2.)** précise qu'il n'est pas difficile de trouver la page d'accès à la base de données en question ; il suffirait d'insérer les bons mots clefs dans le moteur de recherche de Google. Internet serait un espace public ; il serait illusoire de croire qu'on pourrait cacher certaines pages sur ce réseau ouvert.

X.) explique à l'audience qu'au mois de décembre, il avait eu un rendez-vous d'urgence auprès du service médico-sportif de (…) pour renouveler son « Médico » afin de pouvoir jouer au volleyball. Il aurait ainsi été ajouté comme dernier patient de la journée. Il devait se déshabiller, puis attendre une dizaine ou quinzaine de minutes dans une salle. Etant formé en informatique de gestion (*Wirtschaftsinformatiker*), les aspects informatiques attireraient tout particulièrement son attention. Son regard aurait donc été attiré sur un post-it apposé sur un ordinateur portable, post-it qui aurait été aisément visible. Il aurait pensé dans un premier temps qu'il s'agissait du *login* pour l'ordinateur portable en question. Lors de l'examen médical, il aurait cependant constaté que l'assistante se servait de ce mot de passe pour encoder ses données dans la base de données du service médico-sportif.

Il aurait déjà eu antérieurement connaissance de l'existence de cette base de données. Dans le cadre de son engagement pour son club de volleyball, il aurait vu que les certificats d'aptitude envoyés au club indiquent en en-tête l'URL de la base de données afférente.

Son intention aurait été ensuite de vérifier si ses données médicales étaient sécurisées ou non.

Il admet avoir accédé à la base de données une première fois le 5 janvier. Il aurait constaté que l'accès fonctionnait (« *Ech hun gesin : daat geet* »). Il dit avoir été choqué par ce constat.

Il aurait su qu'il allait croiser dans les jours suivant croiser **T2.)** du CIRCL et aurait voulu le lui dénoncer. Il se serait dit qu'il s'agissait bien de l'autorité à laquelle il fallait s'adresser.

Le lundi, il en aurait parlé à un collègue. Celui-ci lui aurait conseillé de consulter un avocat. Sur recommandation, il aurait dans un premier temps cherché conseil auprès de Maître Gaston VOGEL. Celui-ci lui aurait dit que pour sa défense, il devrait s'assurer de pouvoir prouver que l'accès à la base de données était possible. C'est pour se ménager cette preuve qu'il aurait accédé une deuxième fois à la base de données pour réaliser quelques *screenshot* ; « *D'Screenshoten sin entstaanen aus dem Besoin nozeweisen, dass déi faille existéiert huet* ».

Le prévenu **X.)** admet ne pas avoir été très coopératif lors de la perquisition par la police. Il explique son attitude par deux motifs :

- Tout d'abord, les documents de perquisition auraient fait état de crimes comminant des peines allant jusqu'à dix ans. Au vu de son jeune âge, cela l'aurait impressionné et apeuré (« *mir as den Wapp gaangen* »).

- Par ailleurs, le disque encrypté de son ordinateur portable aurait contenu la base de données des membres du parti politique qu'il préside. Il aurait eu peur que cette donnée sensible soit compromise.

Le mandataire du prévenu, Maître Nicky STOFFEL, souligne que son mandant aurait été mu par de bonnes intentions (« *mat guddem Gewëssen* »). Il aurait constaté une faille informatique et l'aurait ensuite dénoncée à l'autorité compétente.

Quant à l'infraction de vol, la défense donne à considérer que l'article 461 du code pénal vise les « choses ». Dans la version applicable au moment des faits, les clefs électroniques n'auraient pas encore été visées par cette disposition. Or, un mot de passe ne tomberait pas dans le champ d'application de cet article :

- Tout d'abord, la jurisprudence préciserait que la soustraction supposerait un appauvrissement dans le chef d'une personne au profit d'une autre.

- La jurisprudence serait également claire en ce que les « choses » ne visent que les meubles corporels. Il faudrait en particulier rapprocher l'article 461 de l'article 505 du Code pénal, qui viserait les choses et les biens incorporels ; a contrario, le concept de choses exclurait les biens incorporels aux yeux du législateur. Elle invoque le principe d'interprétation restrictive du droit pénal.

- Par ailleurs, l'intention frauduleuse ne serait pas non plus donnée. **X.)** aurait voulu dans un premier temps vérifier la réalité de la faille et dans un second

temps vérifier si suite à sa dénonciation, elle avait été réparée. Il n'y aurait ni volonté de nuire, ni volonté de s'enrichir.

Quant à l'infraction à l'article 509-1 du Code pénal, la défense déclare ne pas contester qu'il y a eu un « accès » à une base de données. **X.)** fait cependant plaider que cet accès n'a duré que 5 ou 6 minutes ; on ne pourrait y voir un « maintien » dans un système informatique. Par ailleurs, la loi exigerait un dol spécial à titre d'élément moral. Or, l'intention de nuire ne serait pas non plus donnée en l'espèce.

Quant à une éventuelle violation de la législation sur les droits d'auteur, Maître Nicky STOFFEL fait valoir que d'après l'article 1er de cette loi, les informations seraient exclues de son champ d'application. En outre, le texte exigerait un élément moral spécifique (« sciemment »), ce qui équivaudrait à une intention méchante. Or une telle intention n'aurait pas existé en l'espèce.

La défense conclut ainsi à l'acquittement. A titre subsidiaire, il y aurait lieu d'accorder la suspension du prononcé, sinon de se limiter à une simple amende.

Le représentant du **Ministère public** estime que l'attitude de **X.)** à l'audience montrerait qu'il aurait pris conscience d'être allé trop loin. Il comprendrait que dans un premier temps, il ait accédé à la base de données pour s'assurer de l'existence d'une faille. Après la dénonciation aux autorités, plus rien n'aurait cependant justifié un tel accès.

Quant au vol libellé sub 1), le représentant du Ministère public donne à considérer qu'une clef électronique est quelque chose de réel. Par « chose », il faudrait entendre tout ce qui a une existence réelle et qui n'est pas une « personne ». Toute information serait une chose. L'article 461 du Code pénal ne distinguerait pas entre les choses corporelles et les choses incorporelles.

L'accusation se réfère en particulier à un arrêt de la Cour de Cassation du 3 avril 2014. Elle en tire l'enseignement d'un côté que le vol de biens immatériels est possible, et que par ailleurs le fait de réaliser une photocopie constituerait un vol.

Quant à l'intention frauduleuse, elle serait donnée, étant donné que **X.)** aurait eu parfaitement conscience que le mot de passe n'était pas le sien (« *Hien wosst, dass daat nët him gehéiert huet* »).

Concernant l'infraction libellée sub 4), le représentant du Ministère Public estime dans un premier temps que la chambre du conseil aurait outrepassé ses propres attributions et sa propre ligne jurisprudentielle en substituant à la qualification juridique du réquisitoire une autre. Tout au plus, elle aurait pu prévoir un libellé subsidiaire, mais en tout état de cause, ce ne seraient que les faits qui sont renvoyés. Pour le Ministère Public, le fait afférent constituerait un vol avec fausses

clef. La compétence de la chambre correctionnelle serait donnée, étant donné que la chambre du conseil aurait « pour le surplus », statué conformément au réquisitoire, donc retenu des circonstances atténuantes permettant de procéder à la décriminalisation.

Concernant l'infraction à l'article 509-1 du Code pénal, cette infraction serait à retenir, tant en ce qui concerne l' « accès » qu'en ce qui concerne le « maintien ». L'intention frauduleuse serait donnée, étant donné qu'elle consisterait simplement dans le fait d'accéder tout en sachant qu'on n'y a pas le droit. L'intention de nuire serait couverte par d'autres dispositions.

QUANT AUX INFRACTIONS

1. Vol d'un nom d'accès et d'un mot de passe

Le Ministère Public reproche à **X.)** de s'être rendu coupable de vol en ayant *« soustrait frauduleusement au préjudice du Dr. **D.)** et du Ministère des Sports, les informations d'accès et codes d'accès à la base de données du Service médico-sportif SPMED du Ministère des Sports, à savoir le nom d'accès '**ABC.)**' et le mot de passe '**ABCD.)**', partant des choses ne lui appartenant pas, en les photocopiant à l'aide de son téléphone mobile IPHONE 4 d'un 'post-it' collé sur l'ordinateur mis à disposition du Dr. **D.)** par le Ministère des Sports ».*

Les faits sont censés s'être déroulés à (…) ou à (…), donc dans l'arrondissement judiciaire de Diekirch. Au vu de la connexité avec les autres faits reprochés au prévenu, et qui sont localisés dont l'arrondissement de Luxembourg, la chambre correctionnelle est territorialement compétente pour connaître de ces faits.

Il n'est pas contesté, en fait, que **X.)** s'est servi de son téléphone portable pour photographier le post-it en question. Il convient de qualifier pénalement ces faits.

L'infraction de vol a été étendue dans son champ d'application par une loi du 18 juillet 2014. La loi pénale la plus douce étant la loi pénale la plus restrictive, il convient d'appliquer en l'espèce l'article 461 du Code pénal dans sa teneur applicable au moment des faits.

L'article 461 se lisait comme suit : *« Quiconque a soustrait frauduleusement une chose qui ne lui appartient pas est coupable de vol »*.

• **Interprétation historique**. L'approche historique ne permet que de tirer des conclusions limitées. Si les valeurs immatérielles n'étaient pas entièrement inconnues à l'époque où l'infraction de vol a pris sa forme actuelle, elles ne revêtaient cependant pas l'importance qu'elles ont actuellement.

• **Interprétation grammaticale**. L'article 461 du Code pénal vise la « soustraction » d'une « chose », n'« appartenant » pas à l'accusé. L'interprétation de la notion de « chose » doit se faire aussi au regard des notions d' « appartenance » et de « soustraction ».

Vu le terme **« appartenance »,** le vol ne peut porter que sur des choses susceptibles d'appartenir à quelqu'un. L'appartenance, même à admettre qu'elle ne vise pas que le droit de propriété, doit pour le moins être un rapport de droit qui établit un droit d'exclusivité univoque d'une personne sur cette « chose », donc un monopole permettant d'exclure autrui de la jouissance de cette « chose ».

Ainsi, le vol ne saurait porter sur toute « information » quelconque, étant donné que les informations ne sont en principe susceptibles ni d'appropriation (donc d'être l'objet d'un droit de propriété), ni d'appartenance. Ce n'est que selon certains critères spécifiques, et en général avec un formalisme suppléant à la fonction que la *possession* assume dans le monde tangible, que certaines informations peuvent devenir le monopole d'une personne déterminée qui peut exercer sur elles des prérogatives exclusives proches d'un droit de propriété ; il s'agit des cas de propriété intellectuelle, tels les droits d'auteur, droit de marques, brevets modèles et dessins, etc.

A part ces hypothèses, il n'existe pas de cadre législatif qui déterminerait à qui appartiennent des valeurs ou biens incorporels et qui conféreraient un droit d'exclusivité.

En particulier, un mot de passe est éventuellement 'attribué' à une personne, mais il ne lui appartient pas. Dans la logique de l'accusation, se poserait inévitablement la question de savoir si le docteur **D.)** était toujours en « possession » du mot de passe ou si, en l'affichant à la vue d'un grand nombre de personnes, elle avait déjà perdu toute emprise et tout monopole sur le code d'accès, de sorte que celui-ci était déjà « perdu » et ne pouvait donc plus être « soustrait ».

Il faut encore constater qu'une « information » telle qu'un identifiant et un code d'accès, n'est pas susceptible de « **soustraction** », notion qui suppose un appauvrissement (lat. *sub-trahere ;* sous-tirer, enlever par le bas). Or, le Code d'accès était toujours à disposition du médecin. Suivre la logique de l'accusation amènerait à se poser la question de savoir si **X.)** a volé deux fois la même chose, vu qu'il a pris deux photos du post-it. De manière plus générale, une chose pourrait être volée à d'innombrables reprises à un même « propriétaire » sans que celui-ci n'en soit dépossédé.

Comme l'a souligné le Conseil d'Etat, un vol d'informations ne saurait être assimilé d'office à une atteinte patrimoniale : « *il semble qu'il faille raisonner en cette matière plutôt en termes de possibilité d'atteinte patrimoniale, alors que la captation illicite de données ou d'informations n'aura le plus souvent pas de portée dommageable*

immédiate et effective, celle-ci n'étant le résultat que de l'usage qui sera fait des données et informations illicitement captées » (Projet de loi n° 4641, Avis du Conseil d'Etat du 2 mai 2000, p. 20).

Pour le cas particulier des codes d'accès, il se pose également la question de savoir s'ils relèvent des « biens » qui sont dans le commerce, ou si le mot de passe est plutôt à considérer comme un droit attaché à la personne.

• **Interprétation systématique.** Le législateur étant supposé faire une œuvre cohérente, il y a également lieu d'interpréter l'article 461 du Code pénal dans son contexte, c'est-à-dire au regard des autres normes de la législation luxembourgeoise et de leur terminologie.

A ce titre, il y a lieu de constater que l'article 461 CP est le premier article du Titre IX intitulé « Crimes et délits contre les propriétés ». Or, la propriété est une notion clairement définie et délimitée par notre législation ; elle porte sur les « choses » (Art. 544 CCiv), qui est une notion moins vaste que celle de « bien » utilisée et détaillée aux articles 516 et suivants du Code civil. L'ensemble de ces dispositions se caractérisent par une distinction rigoureuse entre les « biens » et les « choses ».

S'il est vrai qu'en principe, le droit pénal jouit d'une certaine autonomie et que les concepts du droit civil ne s'imposent pas rigoureusement lors de l'interprétation du droit pénal, il faut cependant constater que le Code pénal a fait sienne la distinction terminologique entre les « choses » et les « biens » :

- L'article 505 sur le recel vise les « choses ou les biens incorporels »
- L'article 498 sur la tromperie précise que cette infraction s'applique « aux biens mobiliers y compris incorporels »

L'analyse terminologique des deux codes permet de constater que les « biens » visent une catégorie corporelle et incorporelle, tandis que les « choses » se cantonnent au domaine du corporel.

• **Interprétation téléologique**. La loi est l'expression de la volonté générale, exprimée dans son cadre constitutionnel par le pouvoir législatif. Il convient dès lors de l'appliquer en prenant en considération les intentions du législateur.

Lorsque les délits en matière informatique ont fait leur entrée dans notre législation, il avait été envisagé dans un premier temps d'adapter l'infraction de vol et de compléter l'article 461 du Code pénal comme suit : *« Est assimilé au vol, le fait d'appréhender frauduleusement un bien immatériel ayant une valeur marchande appartenant à autrui en vue d'un usage ou emploi même momentané »* (Projet de loi n° 4393 tendant à renforcer la lutte contre la criminalité économique et la fraude informatique, Texte du projet, page 2).

Le Conseil d'Etat a vivement critiqué cette approche et a jugé *« préférable de créer des règles spéciales relatives à la fraude informatique »* (Projet de loi n° 4393 précité, Avis du Conseil d'Etat, p. 14). Cette solution connaîtra la faveur du législateur, étant donné que l'article 461 restera inchangé et que les articles 509-1 et suivants du Code pénal ont été introduits par la loi du 15 juillet **1993** tendant à renforcer la lutte contre la criminalité économique et la fraude informatique.

En **2000**, les peines des infractions en matière informatiques ont été relevées sur base de la considération suivante (loi du 14 août 2000) :

> *« Le Conseil d'Etat propose toutefois un relèvement des pénalités encourues. Si la Chambre suit le Conseil d'Etat dans sa proposition de ne pas envisager une répression de la fraude informatique au titre des incriminations traditionnelles du vol, de l'extorsion, de l'abus de confiance et de l'escroquerie, les dispositions actuelles de l'article 509-1 du Code pénal permettant de l'appréhender, même si ce n'est que de manière indirecte, encore faut-il alors prévoir des pénalités qui soient suffisamment dissuasives »* (Projet de loi n° 4641/05 relatif au commerce électronique, Rapport de la Commission de l'économie, de l'énergie, des postes et des transports du 10 juillet 2000, p. 30).

Le législateur s'était en effet laissé guider par l'idée que :

> *« les valeurs nouvelles que constituent les biens dits informationnels ou informatiques peuvent être l'objet d'atteintes au même titre que les biens matériels traditionnels. Or, force est de constater que les infractions classiques sanctionnant l'atteinte contre les biens, en particulier le vol, l'abus de confiance ou l'escroquerie, de même que l'extorsion ou le recel, présupposent la matérialité de l'objet du délit »* (Projet de loi n° 4641, Exposé des motifs, p. 28).

Par une loi postérieure aux faits reprochés à **X.)**, le législateur a encore étendu la notion de vol qui peut désormais porter sur « une chose *ou* une clef électronique ». Or, si dans l'intention du législateur, les choses englobaient toutes les valeurs immatérielles, cette ajoute n'aurait pas été nécessaire.

Il découle de ce qui précède que le législateur n'a pas souhaité étendre le vol au-delà des biens matériels, mais a préféré créer des infractions spécifiques.

A cela s'ajoute qu'admettre que le vol puisse couvrir toute information, voire même tout bien incorporel balayerait encore la subtile gradation des peines mise en place par le législateur en matière d'atteinte à la propriété intellectuelle, selon qu'elle affecte des droits d'auteur (simple amende ; Art. 82 de la loi modifiée du 18 avril 2011 sur les droits d'auteur, les droits voisins et les bases de données), des

modèles ou des droits de marque (amende et emprisonnement jusqu'à 3 ans, Art. 184 et 309 CP) ou des brevets (pas de sanction pénale).

Or, le législateur est supposé avoir fait une œuvre utile ; si aux yeux de la loi, toutes ces atteintes à des valeurs immatérielles étaient de toute manière punies d'un emprisonnement de 5 ans à titre de vol, toutes les autres dispositions deviendraient inutile, superfétatoires et partant inopérantes. Or, rien ne permet d'admettre que le législateur ait voulu créer des dispositions inutiles, sombrant d'office dans les règles du concours avec le vol.

Par conséquent, le législateur a entendu la notion de « chose » comme ne visant que les biens matériels.

• L'ensemble des considérations susmentionnées doivent encore être se mesurer au principe de l'interprétation stricte de la loi pénale, découlant du principe constitutionnel de la légalité des peines. Face aux incertitudes d'interprétation qui viennent d'être évoquées, l'interprétation la plus restrictive et donc la plus favorable au prévenu s'impose au juge pénal.

Le Tribunal constate par conséquent que l'infraction de vol ne saurait porter sur des biens incorporels, tels qu'en l'espèce des informations quant aux modalités d'accès à d'autres informations.

Il convient par conséquent d'**acquitter X.)** :

> *« comme auteur, co-auteur ou complice,*
>
> ***1)** le 5 janvier 2012 vers 17.00 heures au Cabinet médical du Dr. **D.)** à* (…)*, sinon au Service médico-sportif à* (…)*, sans préjudice quant aux indications de temps et de lieux plus exactes,*
>
> *d'avoir soustrait frauduleusement une chose qui ne lui appartient pas,*
>
> *en l'espèce, d'avoir soustrait frauduleusement au préjudice du Dr. **D.)** et du Ministère des Sports, les informations d'accès et codes d'accès à la base de données du Service médico-sportif SPMED du Ministère des Sports, à savoir le nom d'accès '**ABC.)**' et le mot de passe '**ABCD.)** », partant des choses ne lui appartenant pas, en les photocopiant à l'aide de son téléphone mobile IPHONE 4 d'un 'Post-it' collé sur l'ordinateur mis à disposition du Dr. **D.)** par le Ministère des Sports ».*

2. Accès et maintien frauduleux dans un système informatique

Il est reproché au prévenu **X.)** d'avoir accédé et de s'être maintenu frauduleusement dans un système de traitement ou de transmission automatisé de données, et ce tant en date du 5 janvier 2012 qu'en date du 9 janvier 2012.

A l'audience, le prévenu **X.)** ne conteste pas avoir accédé à deux reprises à la base de données SPMED. Ces aveux sont confirmés par les éléments objectifs de l'enquête de police.

L'article 509-1 du Code pénal incrimine quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données.

Les serveurs du CTIE, avec les bases de données qu'ils gèrent et les accès à distance qu'ils proposent, forment un système de traitement et de transmission automatisé de données.

Il y a eu en l'espèce un accès, étant donné que le prévenu **X.)**, en se servant de son ordinateur, a établi une connexion avec les serveurs gérant la base de données SPMED, s'y est connecté et a lancé différentes requêtes.

Quant à la notion de « maintien », il convient de constater que celle-ci *« vise à sanctionner l'auteur qui aurait accédé de bonne foi et par inadvertance à un système informatique sans disposer de l'autorisation nécessaire puis se serait maintenu dans ledit système après avoir eu conscience du caractère illicite de l'intrusion »* (LEROUX Olivier, Criminalité informatique, in : Les infractions contre les biens, Larcier 2008, p. 414).

En l'espèce, **X.)** est « resté » sur le site, après avoir accédé de manière non autorisée, il ne s'est pas « maintenu » après un accès autorisé ; le « maintien » ne peut dès lors être retenu à sa charge.

Quant à l'élément moral, l'article 509-1 exige outre le dol général également un dol spécial, à savoir que l'accès doit avoir été fait « frauduleusement », donc dans une intention frauduleuse. En l'espèce, **X.)** savait qu'il n'était pas habilité à accéder à la base de données en question et s'est néanmoins volontairement connecté ; il a dès lors agi dans une intention frauduleuse. Le mobile sous-jacent au passage à l'acte est à ce titre indifférent et ne rend pas l'accès légitime.

Le prévenu **X.)** est par conséquent **convaincu** :

« le 5 janvier 2012 vers 22.00 heures à (…)***,***

2) d'avoir, frauduleusement, accédé dans un système de traitement et de transmission automatisé de données,

en l'espèce, d'avoir accédé frauduleusement dans une partie du système de traitement et de transmission automatisé de donnes de l'Etat, en l'espèce dans la banque de données SPMED du Ministère des Sports et d'y avoir effectué des recherches au sujet des noms « X.) », « A.) », « B.) », « B'.) » et « C.) », ainsi qu'au sujet des personnes « X.) », « E.) » et « G.) »,

3) le 9 janvier 2012 vers 17.00 heures à (…)***,***

d'avoir, frauduleusement, accédé dans un système de traitement et de transmission automatisé de données,

en l'espèce, d'avoir accédé frauduleusement dans une partie du système de traitement et de transmission automatisé de donnes de l'Etat, en l'espèce dans la banque de données SPMED du Ministère des Sports et d'y avoir effectué des recherches au sujet des personnes « X.) » et « C.) ».

3. Affichage, copiage et transmission de fiches médicales

D'après le réquisitoire du Ministère Public, il est reproché au prévenu **X.)** d'avoir, entre le 5 janvier 2012 et le 9 janvier 2012, affiché et copié sur son ordinateur des fiches médicales. L'ordonnance de la chambre du conseil reprend l'affichage et le copiage des fiches et ajoute encore le fait d'avoir « transmis » ces fiches.

Ces faits en tant que tels sont établi au vu des aveux du prévenu et des éléments prédécits du dossier répressif.

Il appartient à la juridiction du fond de donner aux faits dont elle est saisi leur juste qualification juridique.

• **Vol ou vol aggravé**. Les Ministère Public estime que la qualification de vol avec effraction s'impose.

Dans un premier temps, il convient de déterminer si le tribunal est compétent *ratione materiae* pour connaître de cette infraction. La chambre du conseil n'ayant pas envisagé, et même écarté cette qualification dans sa décision, on ne saurait pas non plus admettre qu'elle aurait retenu des circonstances atténuantes pour procéder à la décriminalisation.

Or, il y a lieu de relever que la circonstance aggravante faisant du vol un crime, à savoir l'usage de fausses clefs, peut être exclu en l'espèce. A supposer qu'il y ait eu

usage de fausses clefs, ces fausses clefs n'ont en tout cas pas été utilisées pour ouvrir une maison, un édifice, une construction, un bateau, un wagon, une voiture, une armoire ou un meuble fermé (Art. 484 et 487 *in fine* CP).

Le Tribunal est par conséquent compétent pour connaître de la qualification pénale de vol proposée par le Ministère Public.

Or, tel que détaillé ci-avant, le vol ne porte que sur des biens matériels. Les fiches médicales constituaient en l'espèce des données numériques non matérialisées sur un support.

La qualification de vol est par conséquent à écarter.

• **Atteinte aux droits sur base de données**. Dans son ordonnance, la Chambre du conseil entend voir les faits qualifiés d'infraction à l'article 82 de la loi modifiée du 18 avril 2011 sur les droits d'auteur, les droits voisins et les bases de données.

Le prédit article incrimine notamment *« quiconque, sciemment, vend, offre en vente, importe, exporte, fixe, reproduit, communique, transmet par fil ou sans fil, met à la disposition du public et de manière générale, met ou remet en circulation, à titre onéreux ou gratuit … une base de données sans autorisation … du producteur de base de données ».*

La législation sur la propriété intellectuelle protège sous certaines conditions des créations de l'esprit en conférant un monopole ; elle accorde notamment aux producteurs de bases de données un droit qualifié de « sui generis ».

Sont des bases de données, *« les recueils ou complications d'œuvres ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou d'une autre manière »* (Art. 1 (2) de la loi du 18 avril 2011).

En l'espèce, les données du SPMED forment une compilation d'éléments indépendants accessibles par des moyens électroniques, et donc une base de données au sens de la prédite loi.

La base de données SPMED est constamment mise à jour, de sorte que le délai de protection de 15 ans (Art. 69 de la loi du 18 avril 2011) n'a pas encore expiré.

L'article 67 (3) al. 3 de la loi précise que *« pour autant qu'elles soient licitement rendues publiques, les bases de données appartenant à l'Etat peuvent être copiées dans leur intégralité dans les conditions fixées par règlement grand-ducal »* ; ledit règlement grand-ducal n'a pas encore été pris. En l'espèce, la base de données SPMED a été licitement rendue accessible à un certain nombre d'usagers (les

médecins et leurs assistants), mais n'est pas accessible au grand public. Cette exception ne trouve dès lors pas application en l'espèce.

La base de données SPMED est partant une base de données relevant du monopole de son producteur.

Comme producteur, il y a lieu de considérer *« la personne physique ou morale qui prend l'initiative et assume à titre principal le risque d'effectuer les investissements nécessaires à la création d'une base de données »* (Art. 67 (2) de la loi du 18 avril 2011).

Le service médico-sportif est organisé par le ministre ayant le sport dans ses attributions (Règlement grand-ducal du 8 février 2012 concernant le contrôle médico-sportif obligatoire des membres licenciés actifs des fédérations sportives agréées ; le règlement grand-ducal du 26 août 1980, applicable au moment des faits, retient le même principe). Les Ministères n'ayant pas de personnalité morale propre, il y a lieu de considérer l'Etat comme étant le producteur de la base de données SPMED.

Il n'y a eu en l'espèce aucun accord de la part de l'Etat pour que **X.)** accède à la base de données SPMED.

L'article 82 précité n'incrimine pas la simple consultation non autorisée d'une base de données.

En l'espèce, **X.)** a enregistré diverses données sur ses propres supports informatiques et a envoyé ces données par courrier électronique au vice-président du parti pirate.

Il y a par conséquent eu une opération de « reproduction », de « communication », de « transmission par fil et sans fil » et de « mise en circulation ».

Cet acte doit avoir porté sur une « base de données ». En l'espèce, ont été enregistrés et transmis :

- un fichier représentant l'électrocardiogramme de **X.)**
- quatorze (14) captures d'écran (*Screenshot*). Le Tribunal constate que 13 fichiers se rapportent exclusivement à la fiche de **X.)**. La dernière est un extrait de l'agenda du service médico-sportif.

Or, tel que détaillé ci-avant, la base de données se définit comme étant une « compilation d'éléments indépendants ». Si un sous-ensemble d'une base de données peut à son tour être une base de données, l'extrait tiré d'une seule fiche de la base de données, ou des éléments simplement isolés ne constituent pas en soi

une base de données. Les *screenshots* ne sont pas non plus « disposés de manière systématique », ni « individuellement accessibles ».

Les informations que **X.)** a enregistrées et distribuées ne constituent donc pas une « base de données » en soi, tel que l'exige l'article 82 de la loi du 18 avril 2011.

Il y a par conséquent lieu d'**acquitter** le prévenu **X.)** :

« comme auteur, co-auteur ou complice,

entre le 5 janvier 2012, 22.00 heures et le 9 janvier 2012, 18.00 heures à (…)*,*

***a)** d'avoir soustrait frauduleusement une chose qui ne lui appartient pas,*

*en l'espèce, d'avoir soustrait frauduleusement au préjudice du Ministère des Sports et notamment de **C.)** les fiches médicales concernant **X.)** et **C.)** et contenues dans la banque de données SPMED du Ministère des Sports, partant des choses ne lui appartenant pas, en les affichant et en les copiant sur son propre ordinateur personnel,*

***b)** d'avoir sciemment vendu, offert en vente, importé, exporté, fixé, reproduit, communiqué, transmis par fil ou sans fil, mis à la disposition du public et de manière générale, mis ou remis en circulation, à titre onéreux ou gratuit, une œuvre, une prestation ou une base de données sans autorisation de l'auteur, du titulaire des droits voisins ou du producteur de base de données,*

*en l'espèce d'avoir affiché et copié sur son propre ordinateur personnel les fiches médicales concernant **X.)** et **C.)** contenues dans la banque de données SPMED du Ministère des Sports et d'avoir transmis les fiches médicales concernant **X.)** à **M.)**, sans autorisation du Ministère des Sports ».*

QUANT A LA PEINE

Les délits retenus à charge de **X.)** ont eu lieu à des dates différentes et ont donc nécessité chacun une nouvelle résolution criminelle ; ils sont par conséquent en concours réel entre eux. En application de l'article 60 du Code pénal, la peine la plus forte sera dès lors seule prononcée ; cette peine pourra même être élevée au double du maximum, sans toutefois pouvoir excéder la somme des peines prévues pour les différents délits.

L'infraction à l'article 509-1 alinéa 1er du Code pénal est sanctionnée d'une amende de 500 euros à 25.000 euros ou de l'une de ces deux peines.

Il convient en l'espèce de tenir compte du mobile qui a animé le prévenu. Il n'est pas contesté que les études universitaires du prévenu couvrent le domaine informatique et qu'il préside un parti politique qui s'intéresse de près aux questions soulevées par les nouvelles technologies de l'information. Il est dès lors plausible que le premier accès ait eu lieu dans le but de voir s'il y avait réellement une faille de sécurité, avant de la dénoncer à un organisme compétent. Quant au second accès, l'instruction n'a pas permis de clarifier avec certitude s'il a eu lieu pour vérifier si des mesures appropriées avaient été prises pour mettre un terme à la faille, si **X.)** a agi dans le but de se constituer des preuves contre un éventuel reproche ou s'il a agi par simple curiosité.

En tout état de cause, le Tribunal observe que le prévenu n'a pas agi dans le but de nuire au service médico-sportif ou aux sportifs enregistrés dans la base de données.

Les accès ont été relativement brefs et le prévenu n'a consulté que sa propre fiche, ainsi que quelques fiches de personnes de son entourage. Il n'a pas donné aux informations médicales ainsi recueillies une publicité excessive et n'en a pas tiré d'avantage pécuniaire.

X.) n'a pas d'antécédents judiciaires et les regrets qu'il a exprimés à l'audience paraissent sincères.

Au vu de l'ensemble de ces éléments, le trouble causé à l'ordre public est en l'espèce réparé à suffisance par une amende correctionnelle. Il convient d'adapter l'amende aux revenus du prévenu.

PAR CES MOTIFS :

le Tribunal d'arrondissement de et à Luxembourg, **dix-huitième chambre**, siégeant en matière correctionnelle, statuant contradictoirement, **X.)** et son mandataire entendus en leurs explications et moyens de défense, le représentant du Ministère Public entendu en ses réquisitions,

a c q u i t t e **X.)** des infractions non retenues à sa charge,

c o n d a m n e **X.)** du chef des infractions retenues à sa charge à une amende correctionnelle de **CINQ CENTS (500)** euros,

f i x e la durée de la contrainte par corps en cas de non-paiement de l'amende à **DIX (10)** jours,

c o n d a m n e **X.)** aux frais de sa poursuite pénale, ces frais liquidés à 103,87 euros,

o r d o n n e la restitution à leur(s) légitime(s) propriétaire(s) des téléphones portables, ordinateurs portables et toutes autres choses saisies suivant le procès-verbal de perquisition et de saisie n° SPJ-41/2012/JDA19858.12 dressé en date du 4 avril 2012 par la Police grand-ducale, Service de Police Judiciaire, Section Nouvelles Technologies.

Le tout en application des articles 14, 16, 28, 29, 30, 44, 45, 65 et 509-1, du Code pénal, des articles 155, 179, 182, 184, 184, 185, 190, 190-1, 191, 194-1, 195, 196, du Code d'Instruction Criminelle dont mention a été faite

Ainsi fait et jugé par Henri BECKER, président, Christian SCHEER, premier juge et Jean-Luc PUTZ, juge, et prononcé en audience public au Tribunal d'arrondissement de Luxembourg, en présence de Vincent PEFFER, greffier assumé, en présence de Michèle FEIDER, premier substitut du Procureur d'Etat, qui, à l'exception de la représentante du Ministère Public, ont signé le présent jugement.