Jugt no 2154/2012 **not. 28197/10/CD**

étr.
ex.p.

AUDIENCE PUBLIQUE DU 14 JUIN 2012

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 (…) (Belgique),
demeurant à L-(…), (…),

p r é v e n u

en présence de

la société anonyme **SOC1.) S.A.**
établie et ayant son siège social à L-(…), (…), inscrite au Registre de commerce et des sociétés de Luxembourg sous le numéro B (…),

comparant par Maître Rosario GRASSO, avocat à la Cour, demeurant à Luxembourg,

partie civile constituée contre le prévenu **X.)** , préqualifié.

F A I T S :

Par citation du **16 avril 2012** le Procureur d'Etat près le Tribunal d'arrondissement de et à Luxembourg a requis le prévenu de comparaître à l'audience publique du **10 mai 2012** devant le Tribunal correctionnel de ce siège pour y entendre statuer sur les préventions suivantes :

infractions aux articles 509-1, 509-2 et 509-3 du Code pénal.

A cette audience, la vice-présidente constata l'identité du prévenu et lui donna connaissance de l'acte qui a saisi le Tribunal.

Les témoins Laurent SCHROEDER et **T1.)** 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.)** , assisté de l'interprète Rita SCHMIT, fut entendu en ses moyens et explications de défense, lesquels furent plus amplement développés par Maître Claudia MONTI, avocat à la Cour, demeurant à Luxembourg.

Maître Rosario GRASSO, avocat à la Cour, demeurant à Luxembourg, se constitua partie civile au nom et pour compte de la société anonyme **SOC1.)** S.A. contre le prévenu **X.)** , préqualifié, défendeur au civil ; il donna lecture des conclusions écrites qu'il déposa ensuite sur le bureau du Tribunal et qui furent signées par la vice-présidente et par le greffier.

Sur ce, les débats furent suspendus et la continuation fixée au 15 mai 2012, audience lors de laquelle le prévenu **X.)** fut entendu en ses moyens et explications de défense.

Maître Claudia MONTI, mandataire du prévenu, fut entendue en ses moyens.

Maître Rosario GRASSO, mandataire de la partie demanderesse au civil, fut entendu en ses conclusions.

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 qui suit :

Vu le procès-verbal n° SPJ-41/2010/JDA 11241.1-ENPA/SCHL du 15 novembre 2010 établi par la police grand-ducale, Service SPJ, Section Nouvelles Technologies.

Vu le rapport n° SPJ-41/2010/JDA 11241.4-SCHL du 23 novembre 2010 établi par la police grand-ducale, Service de Police Judiciaire, Section Nouvelles Technologies.

Vu le rapport n° SPJ-41/2011/JDA 11241.12-SCHL du 10 juin 2011 établi par la police grand-ducale, Service de Police Judiciaire, Section Nouvelles Technologies.

Vu la citation à prévenu du 16 avril 2012 régulièrement notifiée à **X.)** .

Vu l'ordonnance de renvoi numéro 149/12 de la Chambre du Conseil du 18 janvier 2012.

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

Le Ministère Public reproche au prévenu **X.)** d'avoir frauduleusement accédé et de s'être frauduleusement maintenu dans le système informatique de la société **SOC1.)** S.A., avec la circonstance que cette 'attaque' a déconnecté du réseau aussi bien le *data center* principal que le *data center* de réserve et qu'il en est résulté une altération du fonctionnement du système informatique.

Il lui est également reproché d'avoir intentionnellement, et au mépris des droits de la société **SOC1.)** S.A., entravé et faussé le fonctionnement du système informatique de cette société en provoquant la déconnexion du réseau aussi bien du *data center* principal que du *data center* de réserve.

L'accusation porte enfin sur le fait d'avoir intentionnellement et au mépris des droits de la société **SOC1.)** S.A. introduit des données dans le système informatique de la société **SOC1.)** S.A. et d'avoir supprimé en partie, sinon modifié, les données qu'il contient ou leurs modes de traitement ou de transmission, notamment par le fait de se connecter systématiquement sur tous les équipements les uns après les autres et à en effacer la configuration et le système d'exploitation.

I. Quant aux faits

Les éléments du dossier répressif, l'instruction à l'audience, les déclarations des témoins Laurent SCHROEDER et **T1.)** (ci-après « **T1.)** »), ainsi que les aveux partiels du prévenu ont permis d'établir les faits suivants :

La société **SOC1.)** S.A. est une société luxembourgeoise offrant des services informatiques dans le domaine du transport aérien. D'après ses propres déclarations, elle compte parmi sa clientèle de nombreuses sociétés de transport aérien à travers le monde, y compris l'entreprise nationale **SOC2.)** S.A.. Afin d'offrir ces services, la société **SOC1.)** S.A. gère un centre informatique (*data center*) à (…), ainsi qu'un second centre informatique externe.

Il est également constant en cause que le prévenu **X.)** a suivi des études universitaires en chimie, puis s'est reconverti par diverses formations et diplômes dans le domaine informatique. Il est notamment titulaire du grade de « ***SOC3.)*** *Certified Network Professional* », qualification qui se situe en troisième position de la hiérarchie des compétences reconnues par la société **SOC3.)** quant à la manipulation du matériel qu'elle commercialise (Entry – Associate – Professional – Expert – Architect). Les deux dernières années (2009/2010), il travaillait pour compte d'une société dénommée **SOC4.)** et était en charge notamment de la structure du réseau de certaines institutions européennes.

Le prévenu **X.)** a été embauché à l'essai par la société **SOC1.)** S.A. avec effet au 1er juillet 2010.

Le 11 octobre 2010, le prévenu a fait l'objet d'un licenciement avec préavis et a été dispensé de travailler.

Le 15 novembre 2010, la société **SOC1.)** S.A. a porté plainte auprès de la police grand-ducale. Elle explique qu'il y a eu une intrusion dans ses deux centres informatiques à travers un accès non autorisé ayant eu lieu le 10 novembre 2010. Une personne s'était connectée à leur réseau interne depuis l'extérieur par le biais d'une connexion dite « VPN ». La conséquence des cette intrusion aurait consisté dans le fait que l'ensemble des quelque 50 routers et autres éléments (switch) du réseau de la société ont été rendus inopérants notamment par la suppression de la configuration et du système d'exploitation de l'ensemble de ces machines.

Par conséquent, l'ensemble du réseau de la société **SOC1.)** S.A. ainsi que des applications qui se servent de ces réseaux a cessé de fonctionner. Etant donné que le système téléphonique interne passait également par le réseau, les communications téléphoniques n'étaient plus possibles qu'au moyen des téléphones mobiles. Puisque l'attaque visait tant le centre principal que le centre destiné à servir de solution de rechange en cas d'incident, les applications que **SOC1.)** S.A. mettait à disposition de ses clients cessaient de fonctionner. Il résulte des éléments du dossier que certaines installations localisées à Londres ont également été affectées.

A 3.20 heures, le service de permanence de la société **SOC1.)** S.A. a été averti par **SOC2.)** S.A. de ce que leur système informatique ne fonctionnait plus. Le plaignant précise que la conséquence immédiate a été que les avions ont dû rester à terre. L'ensemble des personnes disponibles, tout comme des collaborateurs externes, ont dû intervenir pour reconfigurer le réseau et réinstaller les systèmes d'opération sur l'ensemble des routers et switch du réseau.

A 14.30 heures, le réseau fonctionnait à nouveau normalement. A 16 heures, les applications desservant la clientèle étaient à nouveau opérationnelles. Un ingénieur a été dépêché à Londres pour y effectuer les opérations nécessaires.

T1.) , qui travaillait à l'époque en tant qu'ingénieur « réseau et sécurité » auprès de **SOC1.)** S.A., a confirmé à l'audience ce déroulement de l'incident. Il a précisé qu'il fallait environ 1 heure de travail par router ou switch pour le reconfigurer.

L'existence de l'incident même et les conséquences qu'il a eues sur le fonctionnement du réseau de **SOC1.)** S.A. est établi par les données fournies par la partie plaignante, par les enquêtes menées par la police, et n'est par ailleurs pas contesté par la défense.

1. Accès au système informatique

1.1. Eléments du dossier et de l'instruction

L'enquête de police, tout comme l'instruction à l'audience a permis d'arriver aux conclusions suivantes :

(a) Le prévenu avait mis en place le jour du licenciement un accès depuis l'extérieur vers le réseau de son employeur.

Il est constant en cause que le prévenu pouvait accéder depuis l'extérieur vers le réseau de son employeur sous l'identifiant « network ».

La partie plaignante soutient que, bien qu'il ait disposé de cet accès, il n'avait aucun motif pour s'en servir étant donné que durant la période d'essai, **X.)** n'aurait pas encore participé aux services d'astreinte et n'était dès lors pas appelé à intervenir à distance en cas d'incident. Le prévenu par contre soutient avoir été formellement invité – et ce sans que des heures supplémentaires ne lui aient été payées – à travailler durant les fins de semaine, ce qui impliquait également qu'il accède à distance au réseau de l'entreprise. Aucun élément du dossier ne permet de trancher entre ces deux affirmations opposées.

Il résulte toutefois des éléments du dossier répressif que l'accès au réseau de la société **SOC1.)** a été réalisé à travers un compte interne portant le nom d'utilisateur « network2 ». Il s'est avéré que ce compte a été créé par un utilisateur « *admin**X.)***», qui n'est autre que le prévenu. Ce compte a été créé à 13.13 heures le jour de son licenciement.

T1.) précise lors de son audition par la police qu'il s'agit d'un compte du groupe d'administrateurs, donnant accès à l'intégralité du réseau. Normalement, les droits d'accès des comptes VPN donnant un accès depuis l'extérieur seraient cependant toujours limités. Il affirme de même que personne n'aurait été au courant de l'existence de ce compte « network2 ».

T1.) soutient à l'audience que ce compte aurait été créé de manière non autorisée, et sans nécessité aucune. Il conteste avoir été d'une quelconque manière, que ce soit de manière orale ou par une notification automatique, informé de la création de ce compte d'accès.

Le prévenu **X.)** soutient que sa hiérarchie aurait été au courant de la création de ce compte « network2 ». Lors de son audition par la police, il affirme avoir informé oralement les collègues de son équipe. A l'audience, il soutient que le fait de créer un tel compte générerait automatiquement un email de notification adressé à sa hiérarchie, qui aurait dès lors nécessairement été informée de l'existence de ce compte.

Le prévenu ne conteste pas s'être servi du compte « network2 » pour accéder au réseau de son ancien employeur.

Quant à la raison de la création de ce compte, **X.)** soutient depuis le début de l'enquête qu'il n'aurait pas été au courant du licenciement qui allait intervenir le jour même. Pour le surplus, il fournit les explications suivantes :

- Lors de sa première audition par la police, il a déclaré qu'il « s'agit là d'un compte utilisateur disponible à toutes les personnes compétentes de la **SOC1.)** S.A. » pour préciser en suite qu'il s'agirait d'un « 'backup VPN' de mon compte utilisateur principal ». Il est d'avis qu'il a signalé la création de ce compte à son équipe. Le fait que ce compte ait été créé le jour même du licenciement relèverait de la simple coïncidence.

- Lors de sa seconde audition par la police, il estime de même avoir informé oralement ses collègues de travail de la création de cet accès.

S'il est vrai que le licenciement est intervenu après l'installation de ce compte d'accès, le prévenu avait cependant déclaré devant le Juge d'Instruction : « *l'ambiance avec Monsieur **A.)** s'est dégradée. Il m'a dit plusieurs semaines à l'avance qu'il allait mettre fin à mon contrat en période d'essai. Je n'avais juste aucune idée du moment précis qu'il allait choisir pour mettre fin à mon contrat* ».

(b) Le prévenu a accédé au système informatique de son employeur

L'adresse IP de la connexion utilisée pour accéder au réseau de la société **SOC1.)** S.A. est le « (…)». Les données saisies auprès du fournisseur d'accès LUXEMBOURG ONLINE S.A. ont permis de constater que cette adresse IP était affectée, au moment des faits, à l'abonnement souscrit par **X.)** .

La partie plaignante a également informé les enquêteurs que l'utilisateur qui s'est procuré un accès s'est identifié en tant que « SN(…) ». La perquisition effectuée par la suite au domicile du prévenu a permis de saisir un ordinateur portable PACKARD BELL dont le nom d'ordinateur (PCName) consistait dans la simple reprise du numéro de série de ce même ordinateur, à savoir le numéro « SN(…) ».

Il est constant en cause que c'est un compte d'utilisateur dénommé « network2 » qui a servi à accéder via un accès VPN aux serveurs de **SOC1.)** S.A.. Cet état des choses a été confirmé par les données (*log files*) enregistrées auprès de la société **SOC1.)** S.A. et a également pu être retrouvé dans les historiques enregistrés sur l'ordinateur portable privé dont le prévenu s'est servi.

Le témoin **T1.)** confirme à l'audience que le prévenu s'est connecté depuis son ordinateur personnel en utilisant le compte qu'il avait créé le jour de son départ et qu'il s'est ensuite connecté à l'ordinateur utilisé pour l'administration du réseau, à partir duquel il avait accès à l'ensemble du réseau. Le mot de passe pour se connecter à cet ordinateur était connu de toute l'équipe.

Dès sa première audition par la police en date du 23 novembre 2010, le prévenu **X.)** était en aveu d'avoir accédé à plusieurs reprises en date du 10 novembre 2010 aux ordinateurs de son ancien employeur.

(c) Durée et fréquence des accès

L'analyse des données retrouvées sur l'ordinateur du prévenu a permis de constater que ce dernier avait accédé une première fois au réseau de la société **SOC1.)** S.A. le 19 octobre 2010, à 18.05 heures.

D'après les données relevées pour le 11 octobre 2010 par la partie plaignante, le prévenu était connecté par VPN à leur réseau à 8 reprises. Les informations retrouvées sur l'ordinateur du prévenu ont également permis aux enquêteurs de conclure à 8 connexions successives.

D'après les relevés qui figurent au dossier répressif, les premières connexions ont été d'une durée relativement courte. La dernière connexion, débutant à 23.05 heures, a duré près de deux heures. Le temps de connexion total avoisine les 3 heures.

T1.) a indiqué aux enquêteurs de police qu'il ne s'explique pas la raison pour laquelle plusieurs connexions successives ont été faites. Il résulterait toutefois des données que le prévenu s'est à chaque fois déconnecté volontairement de son accès VPN (« déconnexion sur requête de l'utilisateur »).

Lors de son audition du 8 mars 2011, **X.)** remet en question ces données. Il estime s'être connecté tout au plus à quatre reprises ; la plus longue des connexions aurait duré entre 40 et 50 minutes. Il a en outre émis à l'audience l'hypothèse selon laquelle le serveur VPN se serait déconnecté automatiquement après une certaine durée d'inactivité.

(d) Raison de l'accès

Lors de ses auditions par la police, tout comme devant le Juge d'Instruction, le prévenu a déclaré avoir accédé au réseau de son ancien employeur « par simple curiosité » (« *aus purer Neugier* »). Il aurait notamment voulu savoir si ses comptes d'accès étaient toujours actifs.

A l'audience, le prévenu explique qu'il voulait effectivement savoir s'il pouvait encore accéder au réseau de son ancien employeur. Constatant que c'était possible, il aurait passé quelque temps à naviguer sur le réseau « pour retrouver son ancien environnement de travail ». Il aurait ainsi notamment consulté le répertoire qui lui était dédié en tant que salarié et les divers fichiers et documents qu'il avait préparés.

1.2. Conclusion

Au vu des éléments du dossier et des aveux du prévenu, il est établi que ce dernier s'est procuré à plusieurs reprises un accès non autorisé au réseau informatique de la société **SOC1.)** S.A..

2. Opérations informatiques effectuées

2.1. Arguments de la défense

Mis à part l'accès volontaire au réseau de la société **SOC1.)** S.A., le prévenu conteste les autres infractions mises à sa charge. Il dit ne jamais avoir voulu nuire à son ancien employeur. L'incident s'expliquerait du fait qu'il aurait par mégarde lancé un script – c'est-à-dire une succession d'instructions prédéfinie – qui se serait trouvé sur le serveur. Ce script aurait adressé l'ensemble des équipements du réseau et exécuté des commandes qui se sont avérées néfastes.

2.1.1. Explications fournies lors de l'enquête et de l'instruction

Lors de l'enquête et de l'instruction, **X.)** fournit les indications suivantes :

- Lors de sa première audition par la police en date du 23 novembre 2010, **X.)** déclare : « *Je vous confirme donc aussi d'avoir lancé ce script lequel j'ai rédigé/modifié personnellement. Cependant j'étais d'avis que celui-ci ne serait pas achevé et ne fonctionnerait pas correctement … je n'étais certainement pas au courant que ce script aurait comme conséquence un effacement du système d'opération sinon de la configuration de tous les routeurs de la société … je n'ai d'ailleurs pas pris une quelconque influence sur le fait que le lancement du scripte en question fut décalé de plusieurs heures … il s'agit là vraisemblablement d'une configuration par défaut laquelle je ne connaissais pas … j'ai téléchargé le scripte initial de l'internet* ».

- Lors de son audition par la police en date du 8 mars 2011, il soutient : « *Ce script avait initialement à faire des 'back-up' du système d'exploitation des routeurs/switches de notre réseau. Je l'ai lancé accidentellement et sans l'intention de nuire … C'est seulement par après que j'ai consulté ce script et que je me suis rendu compte des conséquences potentiellement néfastes … Afin d'éviter d'autres dégâts, j'ai supprimé le script en question immédiatement* ».

- Lors de son interrogatoire devant le Juge d'Instruction, il précise : « *J'ai ouvert un fichier SCRIPT que je pensais pas achevé. Je précise qu'à mon avis il n'aurait pas dû fonctionner. J'ai été étonné de voir que c'était le contraire … L'un des fichiers était un SCRIPT qui permettait de se connecter au rooter. Je me disais que ce fichier pourrait avoir des conséquences néfastes pour mon ancien patron et je l'ai deleté. Je précise que j'ai ouvert un fichier et je ne savais pas que c'était un script* ».

Lors de son audition par la police, le prévenu a également émis l'hypothèse que l'incident puisse être le fait d'un tiers. Il indique qu'il aurait « un soupçon qu'il y a eu une intrusion illicite dans mon ordinateur portable ». Il affirme que sa carte de crédit a été utilisée abusivement récemment. L'enquête de police révèlera que 8 semaines avant l'incident, le prévenu avait effectivement été victime d'une utilisation frauduleuse de son numéro de carte de crédit, qui est cependant restée à l'état de tentative. Devant le Juge d'Instruction, il réitère

qu'« au vu du nombre de connections et de la durée de celles-ci, je suis d'avis qu'un 'agent extérieur' soit également responsable d'une amplification de ces problèmes ».

2.1.2. Arguments développés à l'audience

2.1.2.1. Explications du prévenu

A l'audience, le **X.)** a déclaré maintenir sa position. Il rappelle qu'il s'est formé en autodidacte. Auprès de son premier employeur, il dit avoir participé à l'administration du réseau du Parlement européen. Il dit avoir changé d'employeur pour rejoindre **SOC1.)** S.A. parce qu'un salaire nettement supérieur lui aurait été offert. Or, la relation avec son supérieur hiérarchique aurait été mauvaise, notamment en raison du non-paiement des heures supplémentaires. Il aurait finalement su qu'il allait être licencié, sans en connaître la date exacte.

Concernant la création du 2e compte d'accès network2, il explique avoir dû le mettre en place en raison de problèmes se présentant avec des télétravailleurs. Il dit avoir eu besoin d'un accès supplémentaire si jamais il y avait un problème avec les comptes de ces derniers. Au moment de la création du compte il n'aurait pas su qu'il allait être licencié le jour même. Il est d'avis que normalement un email est automatiquement envoyé aux membres de son équipe, les informant de la création du compte.

X.) admet s'être connecté une première fois au réseau de son employeur une quinzaine de jours après avoir été licencié, mais il se serait immédiatement déconnecté.

Il admet également s'être connecté le soir de l'incident, mais la connexion aurait été relativement brève et n'aurait pas dépassé une heure. Il dit être entré dans ses dossiers personnels. C'est là qu'il serait tombé sur le script qu'il avait créé à l'époque pour gérer le backup des configurations. Il relèverait de la nature de cette opération que les machines suppriment d'abord leur configuration, avant de recevoir l'instruction de récupérer leur nouvelle configuration à une adresse prédéfinie. Le script aurait probablement contenu une erreur. **X.)** précise – tout en affirmant en avoir fait l'expérience récente auprès de son nouvel employeur – qu'en informatique, la moindre erreur, tel un espace de trop ou une lettre manquante, pourraient conduire à des conséquences inattendues. Ainsi, il aurait décidé de supprimer le script, mais aurait probablement fait un double-click sur le script, causant ainsi son exécution en arrière-fond. Ce n'est qu'ensuite, en visualisant son contenu, qu'il se serait rendu compte de la potentielle dangerosité du script. Il admet avoir copié certaines des instructions dans son éditeur de texte, et ce pour faire ensuite des recherches sur Internet.

Il admet avoir supprimé les fichiers logs pour ne laisser aucune trace de sa connexion.

2.1.2.2. Explications du mandataire

Le mandataire du prévenu expose que ce dernier est en aveu de s'être introduit à plusieurs reprises dans le système informatique de son ancien employeur, et ce en raison d'une « curiosité malsaine ».

Les autres infractions seraient toutefois contestées. La démarche de **X.)** n'aurait pas été volontaire. Le programme en question aurait existé et aurait déclenché un mécanisme qui ne pouvait plus être arrêté. Il s'agirait d'un programme que tout un chacun peut télécharger ; or, l'on téléchargerait souvent d'Internet des choses qu'on ne maîtrise pas. **X.)** n'aurait pas terminé d'adapter le programme, et ne serait dès lors pas encore arrivé au stade auquel il aurait pu tester son fonctionnement. Il aurait fait un excès de zèle en voulant développer des solutions pour des problèmes dont il n'avait pas la responsabilité.

Les diverses apparences et coïncidences résultant de l'enquête seraient insuffisantes pour pouvoir conclure que le prévenu a agi de mauvaise foi. Il ne serait par ailleurs pas exclu non plus qu'un tiers ait utilisé son ordinateur.

En outre, l'ancien employeur du prévenu aurait également fait preuve de négligence en ayant omis de changer de mot de passe après le départ de **X.)** .

2.2. Eléments du dossier répressif et de l'instruction

2.2.1. Quant aux instructions informatiques et au script

(a) Les connections successives qui ont été établies

Dans le cadre de son audition par la police, **T1.)** décrit, en somme, la démarche du prévenu comme suit :

- dans un premier temps, il s'est connecté à distance au réseau de la société **SOC1.)** S.A.,
- au sein de se réseau, il s'est ensuite connecté à l'ordinateur de support, dont il connaissait le mot de passe ; à travers cet ordinateur, il avait accès à l'ensemble de l'infrastructure informatique
- depuis cet ordinateur, des connections ont été faites vers les routeurs et switch composant le réseau.

T1.) précise que ces derniers accès aux routeurs et switch ont été faits « ***un par un*** », et « ceci afin de lancer manuellement sur chaque équipement touché les mêmes commandes néfastes ».

Le prévenu conteste cette affirmation ; tel que détaillé ci-avant, il affirme ne pas avoir exécuté de commandes une par une, mais avoir lancé par mégarde un script exécutant automatiquement ces instructions. Lors de son audition par la police en date du 8 mars 2011, il indique : « Je réfute donc de m'être connecté manuellement à chaque routeur/switch afin de lancer des lignes de commandes ».

L'enquête de police n'a pas permis de retrouver de trace du script que le prévenu dit avoir exécuté.

(b) Provenance et utilité d'un script

Le prévenu soutient avoir téléchargé le script de l'Internet et de l'avoir modifié et transformé par la suite. Il admet notamment l'avoir adapté à la configuration spécifique du réseau de la société **SOC1.)** S.A. en intégrant au script toutes les adresses IP des routeurs et switch.

Le but d'un tel script aurait été de mettre en place un système de back-up des configurations des différents routeurs. Il admet que cela ne lui avait pas été explicitement demandé, mais on aurait exigé de lui d'être « pro-actif », raison pour laquelle il aurait envisagé le développement de nouveaux outils.

A l'audience, le prévenu a réitéré cette même explication.

Lors de son audition par la police, **T1.)** conteste l'utilité de développer un tel script. Tous les outils pour le backup des installations seraient mis à disposition par le fabricant **SOC3.)** sous forme d'un logiciel dénommé « **SOC3.)** Works », permettant d'automatiser les mises à jour.

De même, l'agent Laurent SCHROEDER a expliqué à l'audience qu'il ne relevait pas des fonctions du prévenu de créer un tel script et qu'il existait des solutions internes, notamment deux serveurs dédiés aux backups.

(d) La nature des instructions qui ont été lancées.

L'enquête de police a permis de retracer que les opérations effectuées sur les différentes machines formant le réseau informatique consistaient, schématiquement, en deux étapes :

- dans une première étape, les machines ont reçu instruction d'effacer leurs données de configuration et de vider la mémoire contenant leur système d'exploitation
- dans une seconde étape, les machines ont reçu instruction de redémarrer (« reload ») à 3.21 heures (2.21 UTC) du matin.

Dans un document d'analyse, la société **SOC1.)** S.A. fournit le détail des instructions qui ont été lancées. Il y est notamment fait état d'une instruction très spécifique (« *config-register 0x2142* ») destinée à « forcer les équipements à ne pas utiliser leur configuration ». Les enquêteurs de police précisent dans leur rapport que cette instruction sert à restituer la configuration de la machine concernée dans son état d'origine (« *Werkeinstellung* »).

(e) Individualisation des instructions.

Il est constant en cause que pour que l'attaque informatique telle qu'elle a eu lieu puisse se produire, chaque router et chaque switch doit être adressé individuellement au moyen de son adresse réseau (adresse IP), afin de lui transmettre les instructions à exécuter.

Le prévenu ne conteste pas ce constat, mais affirme que l'ensemble des adresses aurait déjà été intégré au préalable, par ses soins, dans le script dont il affirme ignorer les conséquences exactes.

X.) dit avoir été licencié avant d'avoir pu finaliser le script. Il n'aurait pas eu l'occasion ni de l'analyser en détail, ni de le tester.

Lors de son interrogatoire devant le Juge d'Instruction, il explique que la suppression de la configuration antérieure du routeur faisait partie du processus voulu ; après la suppression, le routeur était censé aller rechercher une nouvelle configuration à partir d'une adresse IP, mais vu qu'il était connecté par son ordinateur privé, les données nécessaires pour permettre au router de se reconfigurer n'aurait pas été disponibles. Ainsi, les configurations auraient été effacées sans être remplacées.

(f) Exécution du script

Le prévenu soutient avoir « lancé accidentellement » le script en question. A l'audience, il fait également état d'un double-click accidentel.

Lors de son audition par la police, le prévenu précise que le script en question avait pour nom «soit « back.pl », soit « script.pl ». Le Tribunal relève que l'extension de fichier « .pl » désigne spécifiquement de tels scripts. Lors de son interrogatoire devant le Juge d'Instruction, il affirme toutefois qu'il aurait « ouvert un fichier et je ne savais pas que c'était un SCRIPT. Là est toute la différence ».

2.2.2. Quant aux données détenues et supprimées

(a) Détention de données sur le réseau informatique (PuTTY client et disque dur externe)

T1.) a précisé lors de son audition par la police qu'un ordinateur professionnel avait été mis à disposition du prévenu.

Sur l'ordinateur portable privé utilisé par le prévenu le jour de l'incident, les agents ont pourtant trouvé un fichier dénommé CCVTTYSetup.exe, qui constitue une application dite « PuTTY Client », logiciel permettant de réaliser certaines connexions entre ordinateurs. L'instruction à l'audience a permis de retenir que ce type de logiciel, tout comme sa présence sur l'ordinateur du portable, n'est en tant que telle pas extraordinaire.

L'enquête a toutefois permis de constater que le logiciel « PuTTY Client » retrouvé sur l'ordinateur du prévenu incluait des données spécifiques relatives à l'infrastructure informatique de la société **SOC1.)** S.A. et du Parlement européen (pour compte duquel le prévenu avait travaillé auprès de son

précédent employeur). Ainsi on y trouvait notamment les adresses de réseau IP de nombreuses machines formant le réseau de **SOC1.)** S.A..

L'analyse d'un disque dur externe saisi au domicile du prévenu a également permis de retrouver deux fichiers reprenant, sous forme schématique, d'importantes parties du réseau informatique de **SOC1.)** S.A.. Il s'agissait des fichiers dénommés « **SOC2.)** -CCS – Lan Logique.vsd » et « **SOC2.)** -CSS – LAN Design 7.5.vsd ».

(b) Fichier texte effacé

Sur l'ordinateur du prévenu, les enquêteurs de police ont encore retrouvé un fichier texte portant le nom « this.txt » qui avait été effacé et transféré par conséquent dans la « poubelle » dans l'attente d'une suppression définitive. Ce fichier texte, qui avait été créé le 10 novembre 2010 vers 20.10 heures, contenait deux instructions informatiques, à savoir :

- « delete bootflash » et
- « squeeze bootflash »

La notion de « bootflash » se réfère à la mémoire dite « flash » sur laquelle est enregistrée la configuration des routeurs et switch d'un réseau informatique. Il s'ajoute en outre que ces commandes informatiques sont spécifiques pour les produits de la marque **SOC3.)** . Leur exécution a pour conséquence la suppression irrévocable de la mémoire du router.

Les agents enquêteurs notent encore que l'exécution de ces commandes doit toujours être confirmée par l'utilisateur (« *dass die beabsichtigte Ausführung der beiden Befehle immer bestätigt werden muss* »). Par conséquent, l'utilisateur qui donne une telle instruction se verra ensuite inviter à confirmer s'il veut réellement exécuter cette action et devra choisir entre « YES » et « NO ». Cette conclusion est confirmée par les dépositions de **T1.)** , qui déclare : « *Afin d'éviter une fausse manipulation éventuelle cette requête doit évidemment être reconfirmée (Are you sur ? : Yes/No)* ».

Lors de son audition par la police, le prévenu avait déclaré : « *Il s'agit là de deux lignes de commandes lesquelles j'ai probablement copiées du contenu du script en question afin de pouvoir rechercher sur l'internet les conséquences de celles-ci. Il n'y a pas d'autres remarques à faire dans ce contexte* ».

(c) Autres fichiers effacés

La partie plaignante avait informé les agents enquêteurs que celui qui avait créé l'accès « network2 » avait également supprimé par la suite les fichiers *log* des serveurs.

Le témoin **T1.)** précise lors de son audition par la police que le prévenu a pris soin d'effacer, au moment de quitter le réseau et avant de se déconnecter, sciemment et irrévocablement les fichiers logs des deux serveurs d'accès VPN (« logserv-lo » et « logserv-vz »). Ce ne serait que dans un autre fichier, relatif à

une autre opération d'authentification, qu'ils auraient réussi à retrouver l'adresse IP de l'intrus.

Lors de son audition par la police, le prévenu a admis avoir supprimé ces données, sans cependant expliquer son geste.

L'analyse de l'ordinateur du prévenu a également permis de constater que le logiciel « **SOC3.)** AnyConnect VPN Client », programme de connexion VPN dont le prévenu s'était servi, avait été désinstallé de cet ordinateur. Seuls quelques fichiers n'avaient pas été effacés, ceux-ci ayant permis aux enquêteurs de retracer les données de connexion.

2.2.3. Eléments contextuels

(a) Activités parallèles

L'analyse des données dites « Cookies » sur l'ordinateur portable utilisé par le prévenu a permis de retracer son historique de navigation sur Internet le soir du 10 novembre 2010. Les agents de police notent qu'il s'est informé notamment sur des appareils spécifiques (« Catalyst-6500 » et « Catalyst3550 ») du constructeur **SOC3.)** . Il s'agit du même type d'installation que celles qui ont été victimes de l'attaque le même soir.

Auprès de la police, **X.)** soutient : « les recherches exécutées sur l'équipement 'catalyst-6500' sont strictement liées à mes besoins professionnels et nullement en relation avec l'intrusion illicite ».

(b) Comportement postérieur du prévenu

Le 10 novembre 2010, vers 23.58 heures, le prévenu a consulté le site internet public de son employeur (« www.**(...)** »), et plus spécifiquement les pages dédiées aux offres d'emploi.

Il résulte de l'enquête de police que l'ordinateur du prévenu a été éteint (« Shutdown Time ») le 11 novembre 2010 à 4.09 heures.

A 8.51 heures du matin, le prévenu a consulté à nouveau le site internet public, et en particulier les pages relatives aux communiqués de presse. Il en fera de même à 17.13 heures.

(c) Infection de l'ordinateur

Le prévenu ayant émis l'hypothèse de l'intervention d'un tiers à travers son ordinateur, les enquêteurs de police ont procédé à des recherches en ce sens. Ils ont constaté dans un premier temps :

- que l'ordinateur avait installé le logiciel d'exploitation WINDOWS XP, dans sa dernière version (Service Pack 3),

- que les mises à jour automatiques du système d'exploitation étaient activées,
- que le pare-feu (Firewall) était activé,
- qu'un logiciel anti-virus était installé, qui était réglé pour se mettre automatiquement à jour,
- qu'enfin, un logiciel contre les applications malveillantes était installé et le dernier contrôle avait été effectué le 11 novembre 2010.

Les agents enquêteurs ont encore procédé à une analyse détaillée du disque dur moyennant le logiciel antivirus installé sur cet ordinateur (« Avast home ») et ont également fait analyser une copie du disque dur par deux autres logiciels anti-virus (« Kapersky Internet Security 2010 » et « avira »). Ces analyses n'ont permis de trouver aucun logiciel malveillant.

Les agents concluent ainsi : « *Eine tatsächliche Kompromittierung des untersuchten Rechners anhand einer eventuellen Schadsoftware konnte somit nicht festgestellt werden* » *et* « *Eine eventuelle missbräuchliche Nutzung … durch eine unbekannte Drittperson des vermeintlich kompromittierten Rechners … wird durch Amtierende aufgrund der gewonnenen Erkenntnisse ausgeschlossen* ».

A l'audience, l'enquêteur Laurent SCHROEDER confirme ces recherches et conclut que l'ordinateur en question était « propre », contrairement à d'autres configurations qu'il leur arriverait de voir.

2.3. Appréciation

Le Tribunal relève que le Code d'instruction adopte le système de la libre appréciation de la preuve par le juge, qui forme sa conviction librement sans être tenu par telle preuve plutôt que par telle autre. Il interroge sa conscience et décide en fonction de son intime conviction (FRANCHIMONT, Manuel de Procédure Pénale, p. 764). Il est de jurisprudence constante que le juge répressif apprécie souverainement, en fait, la valeur probante des éléments sur lesquels il fonde son intime conviction (Cass. belge, 31 décembre 1985, Pas. 1986, I, 549; Cass. belge, 28 mai 1986, Pas. 1986, I, 1186).

Le Tribunal base en l'espèce sa conviction sur les considérations suivantes :

Tout d'abord, l'hypothèse de l'intervention d'une personne tierce qui aurait piraté l'ordinateur du prévenu pour commettre des actes frauduleux ou en amplifier les conséquences est à exclure. Tout d'abord, cette affirmation est restée à l'état de simple allégation, le prévenu n'ayant formulé que quelques vagues hypothèses. Les tentatives d'abuser de sa carte de crédit ne présentent aucun lien avec ses problèmes informatiques, et encore moins avec son employeur **SOC1.)** S.A.. Les services spécialisés de la police grand-ducale ont procédé à une analyse minutieuse de l'ordinateur en question et n'ont trouvé aucun indice permettant de conclure à un piratage de cet ordinateur. En outre, à suivre l'argument de défense invoqué, il faudrait admettre qu'une personne tierce et malveillante ait su que le prévenu allait se servir de l'ordinateur privé de son épouse pour le pirater au préalable, puis attendre jusqu'à ce qu'il se

connecte sur le réseau de son employeur, pour ensuite – usant de connaissances spécifiques quant au réseau de **SOC1.)** S.A. et quant aux infrastructures **SOC3.)** – lancer à l'insu du prévenu diverses opérations néfastes. Cette même personne aurait par la suite effacé toute trace de son intervention, au point que la police grand-ducale n'arrive pas à la détecter. Une telle constellation est à ce point invraisemblable qu'elle doit être écartée et ne saurait créer un quelconque doute raisonnable.

Le prévenu est en aveu de s'être procuré un accès illégitime au système informatique de la société **SOC1.)** S.A.. Dans la mesure où toute intervention d'un tiers est exclue, et que les données trouvées auprès de la société **SOC1.)** S.A. se recouvrent avec celles tirées de l'ordinateur saisi au domicile du prévenu, il est établi qu'il y a eu en tout 8 connexions le 10 novembre 2010, d'une durée cumulée de près de 3 heures.

X.) fournit comme explication sa curiosité notamment quant à la question de savoir si ses anciens comptes d'accès étaient toujours actifs, ainsi que sa volonté de retrouver son ancien environnement de travail. Le Tribunal relève que ces explications ne sauraient convaincre. En effet, il est établi dans un premier temps que le prévenu avait déjà eu accès le 19 octobre 2010. Il savait donc depuis ce moment que ses anciens mots de passe étaient encore valables. Sa curiosité était ainsi assouvie.

De même, même à admettre qu'il ait été pris le soir du 10 novembre 2010 d'un nouvel élan de curiosité, toujours est-il que le prévenu s'est reconnecté pendant près de 3 heures, durée qui ne peut s'expliquer par la simple volonté de vérifier quelques mots de passe et de consulter quelques documents que le prévenu avait rédigés à l'époque où il travaillait pour compte de **SOC1.)** S.A..

Il s'ajoute en outre que le prévenu n'avait pas quitté cette société en bons termes, mais que suite à des différends internes, il avait été mis fin à son contrat, de sorte qu'une nostalgie de retrouver son ancien environnement de travail ne saurait exister. De plus, le prévenu avait copié sur ses supports privés de nombreuses informations quant à l'infrastructure du réseau de son ancien employeur et pouvait donc consulter ces données, si besoin en était, sans devoir se connecter sur l'ordinateur de son employeur.

Le Tribunal retient dès lors que les 8 accès illégitimes au réseau de la société **SOC1.)** S.A. ne sauraient s'expliquer par une simple nostalgie ou curiosité.

Au contraire, le Tribunal relève que le prévenu avait toutes les raisons d'éprouver des ressentiments à l'égard de son ancien employeur. En effet :

- **X.)** avait expliqué à l'audience n'avoir abandonné son ancien poste de travail qu'en raison de la promesse d'un salaire nettement supérieur.
- Il a également expliqué à l'audience que les tâches qui lui ont été finalement attribuées étaient peu intéressantes et nettement en-dessous de ses compétences réelles.
- D'après ses propres explications, les relations avec son supérieur hiérarchique, n'étaient pas bonnes, tant parce que ce dernier doutait de

ses compétences, que parce qu'il refusait de payer des heures supplémentaires que le prévenu estimait dues.
- Enfin, le prévenu a été licencié en période d'essai et avec dispense immédiate de toute prestation de travail.

D'après ses propres explications devant le Juge d'Instruction, le prévenu savait qu'il allait être licencié, même s'il n'avait pas connaissance de la date exacte.

Il est constant en cause qu'avant de quitter son emploi, le prévenu a créé un compte 'network2' lui permettant de bénéficier d'un accès à distance. Les explications - d'ailleurs contradictoires - du prévenu selon lesquelles il y aurait eu une notification orale sinon automatique relative à la création de ce compte ne sont corroborées par aucun élément du dossier. Face aux déclarations de **T1.)** , qui précise que la création de ce compte ne correspondait à aucune nécessité, **X.)** n'a fourni aucune explication convaincante.

Le Tribunal en déduit que la création de ce compte 'network2' ne pouvait avoir d'autre finalité que de se ménager, notamment pour le cas où il serait licencié, un accès caché au système informatique de son employeur.

Pour le surplus, la défense de **X.)** repose essentiellement sur deux affirmations, à savoir :

(a) Le prévenu affirme qu'il existait un script préétabli, mais qu'il ne l'aurait pas mis à exécution volontairement.

(b) Le prévenu affirme ne pas avoir su quel était l'impact du script sur l'installation informatique de **SOC1.)** S.A..

ad (a). Aucun élément du dossier répressif ne vient corroborer l'existence d'un quelconque script.

T1.) estime à l'audience qu'il est peu probable que le prévenu ait utilisé un script. Dans ce cas, l'exécution des différentes instructions aurait été beaucoup plus rapide et n'aurait pris que quelques secondes.

Le prévenu n'a fourni aucune explication convaincante quant à la raison pour laquelle il aurait téléchargé un modèle de script d'Internet, l'aurait partiellement adapté à l'infrastructure de **SOC1.)** S.A. pour ensuite abandonner le projet et laisser un script mi-achevé et potentiellement dangereux sur le serveur.

En particulier, il résulte du témoignage de **T1.)** que non seulement la création d'un système de backup des configurations des routeurs ne correspondait pas aux missions confiées au prévenu, mais encore que des solutions automatisées existaient. Le Tribunal entend accorder crédit à ces déclarations, étant donné qu'il paraît évident qu'un opérateur international tel que **SOC1.)** S.A., tout comme un constructeur mondial tel que **SOC3.)** , ont nécessairement développé des solutions de secours et de backups suffisants et performants et qu'il n'y avait pas lieu de se servir d'un quelconque script téléchargé d'Internet pour créer ou améliorer le backup du système.

Il n'y avait dès lors aucune raison de créer un quelconque script de backup.

Il est par ailleurs fait état dans le dossier répressif de certaines commandes qui ont été directement adressées aux installations via la « console », donc à travers la saisie directe de données, et non à travers une exécution automatisée.

De même, sur base des commandes enregistrées, **T1.)** a confirmé à plusieurs reprises que les commandes ont été insérées une par une.

La durée de connexion de 3 heures n'aurait par ailleurs pas été nécessaire s'il s'agissait simplement de consulter quelques fichiers et de lancer un script ; elle s'explique par contre aisément si le prévenu devait adresser individuellement une quarantaine de machines pour leur faire exécuter une série d'instructions.

Le Tribunal retient dès lors que l'existence du « script » allégué par le prévenu n'est pas à retenir.

S'il est vrai que l'enquêteur de police a confirmé à l'audience qu'un script peut être démarré dans certaines configurations par un simple double-click, il relèverait cependant des plus grand hasards qu'un informaticien chevronné tel que le prévenu **X.)** se trompe d'action et, en voulant ouvrir le document pour consulter son contenu, fasse par mégarde un double-click sur ce document causant ainsi son exécution en arrière-fond.

ad (b). Il s'ajoute, même à supposer que ce script existait, que le prévenu savait nécessairement quel était son impact. Le Tribunal arrive à cette conclusion sur base des éléments concluants et pertinents suivants :

- Le prévenu ne s'est pas simplement connecté au réseau de **SOC1.)** S.A. pour y prendre inspection de l'un ou de l'autre fichier, mais s'est directement connecté par la suite à l'ordinateur de support, dont il savait qu'il lui donnait accès complet à toute l'infrastructure.

- Le prévenu ne conteste pas avoir pris inspection du script au préalable, puisqu'il dit l'avoir modifié en y intégrant notamment toutes les adresses réseau IP de l'installation de son employeur. Il avait dès lors nécessairement également pris connaissance des différentes instructions qu'il contenait.

- Il est constant en cause que **X.)** est un informaticien expérimenté, spécialement diplômé pour les installations **SOC3.)** . Il ne saurait dès lors affirmer qu'il ignorait la portée d'un tel script, ni en particulier le sens et la portée d'instructions telles que « delete bootflash » et « squeeze bootflash », dont l'impact potentiellement néfaste saute aux yeux même d'un novice.

- Le prévenu a également – sauf à supposer que le script téléchargé aurait été spécifique pour les routers **SOC3.)** Catalyst-6500 – lui-même

introduit les commandes « delete bootflash » et « squeeze bootflash », celles-ci étant spécifiques à ce type d'appareil.

- Le fait que les deux instructions néfastes se soient retrouvées dans un fichier texte créé le soir même des faits prouve également que le prévenu n'a non seulement pris connaissance de la présence de ces instructions, mais s'y est même intéressé de près.

T1.) explique qu'en lisant ces opérations, un informaticien spécialisé comprend toute de suite quelles en sont les conséquences. Les instructions « squeeze » et « delete » ne seraient guère nécessaires pour une opération de backup. Par ailleurs, tout informaticien procéderait à des tests des programmes qu'il rédige.

La bonne foi du prévenu **X.)** est par ailleurs ébranlée par le fait qu'il a supprimé une série de fichiers, à savoir :

- Il a supprimé sur deux serveurs les fichiers *log* permettant de retracer les accès à distance par VPN. Le Tribunal en déduit qu'il a cherché à effacer les traces de l'accès qu'il venait de faire. Ce n'est que par hasard qu'une autre trace a pu être retrouvée.
- Il a également mis à la poubelle le fichier texte qu'il avait créé le soir de l'incident et qui contenait les commandes néfastes.
- Le prévenu a de même supprimé sur son ordinateur le logiciel d'accès par VPN.

La suppression de ces éléments ne peut s'expliquer autrement que par le fait que le prévenu connaissait l'impact néfaste des instructions qu'il venait de lancer. Son affirmation – faite dans certaines de ses auditions – selon laquelle il n'aurait appris que bien après l'impact de ce script est ainsi contredite.

L'affirmation du prévenu qui – dans certaines de ses auditions – a affirmé qu'il ne se serait rendu compte que par la suite, donc en consultant le script après l'avoir lancé accidentellement, de l'effet potentiellement néfaste de ce dernier, ne saurait pas non plus convaincre. En effet, dans ce cas, il se serait rendu compte que l'instruction fatale n'allait s'exécuter que vers 3 heures du matin, ce qui lui laissait plusieurs heures pour prendre les mesures nécessaires pour annuler cette commande ou prévenir ses conséquences, sinon pour alerter son employeur de son 'inadvertance'.

L'argumentaire du prévenu est par ailleurs mêlé de contradictions, notamment dans le fait d'affirmer que c'est lui qui aurait par mégarde lancé un script aux conséquences néfastes, mais de soupçonner en même temps l'intervention malintentionnée d'un tiers ayant piraté son ordinateur.

Le Tribunal relève encore qu'il ne résulte d'aucun élément du dossier, tel que le prétend le prévenu, qu'une commande invitant les routeurs à télécharger une nouvelle configuration aurait été lancée mais se serait soldée par un échec.

• Tant le témoin **T1.)** que les enquêteurs de police ont en outre confirmé que des instructions d'une portée telle que celles qui ont été utilisées ne s'exécutent

pas automatiquement et sans que l'utilisateur ne s'en rende compte, mais invitent nécessairement ce dernier à confirmer en tapant « Y » (Yes) que l'exécution de cette commande est réellement souhaitée.

Ainsi, pour chaque routeur et chaque switch, le prévenu a nécessairement été invité à confirmer par une démarche active et consciente qu'il voulait que cette instruction s'exécute. Il ne saurait dès lors argumenter qu'il ne savait pas que le script était en train de s'exécuter, ni qu'il allait supprimer la mémoire et la configuration des différentes composantes du réseau.

Au vu des éléments qui précèdent, il n'est pas seulement établi que l'existence d'un script est des plus invraisemblable, mais que par ailleurs – que ce soit un script ou des instructions individualisées qui ont été exécutées – le prévenu **X.)** avait connaissance de leur portée et a néanmoins individuellement validé par un « YES » leur exécution sur des dizaines de routers et switch.

Pour être complet, le Tribunal relève encore qu'à titre d'élément moral des infractions intentionnelles, le *dolus eventualis* (dol éventuel) est suffisant. Il y a par conséquent dol dès lors que l'auteur a simplement envisagé les conséquences que son acte pourrait avoir.

• Pour former sa conviction, le Tribunal prend encore appui sur les éléments suivants qui ont entouré la commission des faits :

- Il est constant en cause que le prévenu a cherché le soir en question des informations techniques quant aux différentes commandes destinées à contrôler des routeurs **SOC3.)** . Son explication selon laquelle cette recherche aurait simplement servi à des fins de « formation » ne saurait convaincre le Tribunal. En effet, rien n'explique pour quelle raison le prévenu aurait passé ses soirées, tout en étant connecté aux serveurs de son ancien employeur, à parfaire sa formation en matière d'installations **SOC3.)** . Au contraire, il s'agit d'un indice de plus qui démontre que **X.)** s'est informé quant aux effets de certaines instructions qu'il a par la suite exécutées sur le réseau de **SOC1.)** S.A..

- Le fait d'avoir par la suite consulté les communiqués de presse sur le Site Internet de la société **SOC1.)** S.A. ne peut par ailleurs s'expliquer autrement que par la volonté de connaître l'impact qu'a provoqué son intrusion nocturne.

- Le prévenu n'a enfin fourni aucune explication quant à la raison pour laquelle il avait copié, puis conservé tant sur l'ordinateur de son épouse que sur un disque dur externe, des informations détaillées quant à l'architecture du réseau de **SOC1.)** S.A..

• Au vu de l'ensemble de ces considérations, le Tribunal retient pour établi que **X.)** a non seulement accédé au système informatique de son ancien employeur, mais a également volontairement exécuté des instructions répétées dont il savait qu'elles allaient mettre hors service un grand nombre de routers et

switch et provoquer ainsi la mise à l'arrêt du réseau informatique de la société **SOC1.)** S.A..

II. Au pénal

1. Quant aux infractions

L'atteinte a en l'espèce été portée au réseau informatique de la société **SOC1.)** S.A., qui est constitué d'un ensemble de router et switchs connectant entre eux les serveurs de la société et les mettant en relation avec des entreprises à travers le monde, afin de pouvoir gérer les applications et bases de données qui forment le service que cette société vend à ses clients.

L'atteinte a porté dès lors à un système de « traitement » et de « transmission » automatisé de données.

Le prévenu est en aveu d'avoir accédé au système informatique de son ancien employeur ; il s'y est également maintenu pendant une durée de plusieurs heures. Cet accès a été frauduleux, tant parce que **X.)** s'était secrètement créé un compte d'accès que parce qu'il savait qu'après avoir été licencié, il n'avait plus le droit d'accéder au réseau, ni de se servir des mots de passe.

La circonstance aggravante est également donné, étant donné que l'accès du prévenu a provoqué l'arrêt complet du réseau informatique, partant altéré son fonctionnement.

L'infraction à l'article 509-1 du Code pénal, libellée sub 1) est dès lors à retenir à sa charge.

Au vu des faits tels que retenus par le Tribunal, il est également établi que le prévenu a intentionnellement entravé le bon fonctionnement du système informatique de son ancien employeur ; il l'a fait au mépris des droits de son ancien employeur et de ses clients.

L'infraction libellée sub 2) est partant donnée.

Enfin, il est établi que le prévenu :

- a intentionnellement fait exécuter des instructions informatiques sur les différentes composantes du réseau, partant « introduit des données » dans le réseau informatique
- a intentionnellement provoqué la suppression des données de configuration et des systèmes d'exploitation de ces éléments, ainsi qu'effacé divers fichiers, notamment des fichiers log, partant « supprimé des données » contenues dans le réseau.

Il a également influé sur le mode de traitement et de transmission des données au sein du réseau, étant donné qu'en provoquant sa mise à l'arrêt, il a empêché toute transmission et tout traitement de données.

Le dernier des chefs d'accusation est dès lors également à retenir à sa charge.

Sur base du dossier répressif et au regard des développements qui précèdent, le prévenu **X.)** est **convaincu** :

« entre le 11 octobre 2010 et le 10 novembre 2010 dans l'arrondissement judiciaire de Luxembourg, à (…) ***et à*** (…) ***et notamment le 10 novembre 2010 entre 17.55 heures et 22.05 heures à*** (…) ***auprès de la société SOC1.) S.A.,***

comme auteur ayant commis lui-même l'infraction,

1) en infraction à l'article 509-1 du Code pénal,

d'avoir frauduleusement accédé et de s'être maintenu dans un système de traitement et de transmission automatisé de données, avec la circonstance qu'il en est résulté une altération du fonctionnement du système,

en l'espèce, d'avoir frauduleusement accédé et de s'être maintenu dans le système informatique de la société SOC1.) S.A., avec la circonstance que cette 'attaque' a déconnecté du réseau aussi bien le data center principal que le data center de réserve, et qu'il en est en conséquence résulté une altération du fonctionnement du système informatique,

2) en infraction à l'article 509-2 du Code pénal,

d'avoir, intentionnellement et au mépris des droits d'autrui, entravé et faussé le fonctionnement d'un système de traitement et de transmission automatisé de données,

en l'espèce, d'avoir intentionnellement et au mépris des droits de la société SOC1.) S.A. entravé et faussé le fonctionnement du système informatique de la société SOC1.) S.A. en provoquant la déconnexion du réseau aussi bien du data center principal que du data center de réserve,

3) en infraction à l'article 509-3 du Code pénal,

d'avoir, intentionnellement et au mépris des droits d'autrui, introduit des données dans un système de traitement et de transmission automatisé et d'avoir supprimé les données qu'il contient et leurs mode de traitement et de transmission,

en l'espèce, d'avoir intentionnellement et au mépris des droits de la société SOC1.) S.A. introduit des données dans le système informatique de la société SOC1.) S.A. et supprimé en partie les données qu'il contient et leur mode de traitement et de transmission,

notamment par le fait de se logger systématiquement sur tous les équipements les uns après les autres et à en effacer la configuration et le système d'exploitation ; par le fait de supprimer sur les 2 serveurs centralisés les fichiers log ; par le fait de se connecter à une quarantaine de routeurs un par un et de lancer pour chaque routeur les mêmes commandes néfastes effaçant la configuration complète des routeurs/switchs en tapant, sur la console de l'appareil, la commande 'write/erase' et en confirmant à chaque reprise cette commande ; et par le fait de lancer une instruction forçant les équipements à ne pas utiliser leur configuration initiale et de planifier le redémarrage décalé des équipements en cause ».

2. Quant à la peine

Les différentes infractions ont en l'espèce été commises dans un but unique. Bien qu'il s'agisse d'une succession d'accès et de commandes informatiques que le prévenu a lancées depuis son ordinateur portable privé, il ne s'en s'agit pas moins d'une seule opération informatique ciblée. L'accès au système était une condition préalable nécessaire pour la suppression de données, qui a son tour a été nécessaire pour en entraver le bon fonctionnement. Les infractions retenues à charge du prévenu **X.)** sont par conséquent en **concours idéal** entre elles. En application de l'article 65 du Code pénal, la peine la plus forte sera dès lors seule prononcée.

- L'article 509-1 alinéa 2 du Code pénal sanctionne l'accès frauduleux dans un système de traitement de données dont il est résulté une altération du fonctionnement de ce système, d'un emprisonnement de quatre mois à deux ans et d'une amende de 1.250 euros à 25.000 euros.

- Les infractions aux articles 509-2 et 509-3 du Code pénal sont punies d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines.

La peine la plus forte, donc celle à encourir par le prévenu, est celle comminée pour les infractions aux articles 509-2 et 509-3 du Code pénal.

Dans l'appréciation de la peine, il convient de tenir compte de la démarche ciblée et organisée du prévenu. Ses actes avaient pour seul but de nuire à son employeur. **X.)** n'a tiré aucun bénéfice pécuniaire personnel de son acte, de sorte que son geste ne peut s'expliquer que par un désir de vengeance.

Il convient également de prendre en considération les conséquences importantes et néfastes de son geste sur l'infrastructure de **SOC1.)** S.A., qui se sont répercutées sur le bon fonctionnement des entreprises clientes.

Il y a dès lors lieu de condamner le prévenu à une peine d'emprisonnement ainsi qu'à une amende appropriée.

Il s'ajoute que le prévenu connaissait non seulement l'impact des instructions qu'il faisait exécuter dans le réseau de son ancien employeur, mais qu'il avait également connaissance de la nature des activités de son employeur. Il savait dès lors que ce dernier fournissait des services à d'importantes compagnies aériennes, qui avaient besoin des applications réseau en temps réel pour organiser le déroulement de leurs opérations de fret aérien. Il savait donc qu'en agissant comme il l'a fait, il n'empêchait pas simplement la société de son employeur à fonctionner le temps de quelques heures, mais il savait qu'il allait créer à travers le monde d'importants problèmes à de multiples compagnies et créer ainsi un préjudice financier très considérable. Il savait également qu'en agissant ainsi, il allait gravement porter atteinte à l'image de son ancien employeur et l'exposer à des revendications indemnitaires potentiellement importantes. Le fait que – tel que cela s'est avéré à l'audience – la plus grande partie du préjudice a été prise en charge par des assurances, ne saurait atténuer l'importante énergie criminelle dont le prévenu a fait preuve.

Dans l'appréciation de la peine, il convient ainsi de tenir compte de cette volonté de nuire et de maximiser le préjudice matériel causé.

Il convient également de tenir compte de l'attitude du prévenu lors de l'enquête et à l'audience, consistant à nier ses actes, à les mettre au compte d'une anodine négligence et même d'invoquer une co-responsabilité de son employeur consistant à ne pas avoir changé de mot de passe pour éviter des accès frauduleux.

X.) n'a pas présenté d'excuse ni exprimé de regrets à l'audience.

Eu égard à ces éléments, il n'y a pas lieu d'assortir la peine à prononcer d'un quelconque aménagement.

III. Au civil

A l'audience du 10 mai 2012, Maître Rosario GRASSO, avocat à la Cour, se constitua partie civile pour et au nom de la société anonyme **SOC1.)** S.A. contre le prévenu **X.)** .

Cette partie civile déposée sur le bureau du Tribunal correctionnel de Luxembourg est conçue comme suit :

Il y a lieu de donner acte à la demanderesse au civil de sa constitution de partie civile.

Le Tribunal est compétent pour en connaître, eu égard à la décision à intervenir au pénal à l'égard du prévenu **X.)** .

La demande civile est recevable pour avoir été faite dans les forme et délai de la loi.

Dans ses conclusions écrites, la partie civile réclame le montant de 170.344,40 euros avec les intérêts légaux à partir du jour des infractions, jusqu'à solde.

La partie civile déclare à l'audience réduire sa demande à 97.126,85 euros.

Le mandataire du prévenu conteste la demande quant à son quantum.

A l'appui de sa demande, la partie civile verse un document qualifié d'« estimation » dans laquelle elle décompose le montant de 97.126,85 euros comme suit :

a) 4.750 euros en raison du recours à un consultant externe. Elle affirme ne pas avoir de facture puisque ce serait inclus dans le contrat de maintenance.
b) 4.519 euros à titre d'heures supplémentaires pour ses ingénieurs, à savoir 10 personnes à raison de 8 heures au prix de 450 euros par jour et par personne, incluant la majoration pour heures supplémentaires.
c) 941.46 euros pour un vol vers Londres, les frais d'hôtel et autres frais de voyage, conformément à un décompte figurant dans un fichier qui n'est pas versé aux débats.
d) 3.341,99 euros pour le client « **CL1.)** », conformément à une facture contenue dans un fichier qui n'est cependant pas versé en copie.
e) 20.893,60 euros en tant que frais « d'impact interne » (« Internal CHAMP Impact à hauteur de 20.893,60 euros.
f) 62.680,80 euros en tant que pertes de revenus.

ad a) et b). Il découle de la nature même des faits que la société **SOC1.)** S.A. a dû remédier dans l'urgence aux conséquences qui ont été causées. Il résulte du témoignage de **T1.)** ainsi que des déclarations du plaignant que la partie civile a eu recours tant à ses salariés internes qui ont fait des heures supplémentaires, qu'à des intervenants internes.

La demande pour ces postes est dès lors fondée quant à son principe.

Les montants réclamés, contre lesquels aucune critique précise n'a été formulée, ne paraissent pas surfaits, de sorte qu'il convient de les allouer.

ad c). Il résulte du témoignage de **T1.)** que certaines réparations ont nécessité un déplacement à Londres.

Le charge de la preuve du préjudice matériel incombe à la partie demanderesse.

Les frais de voyage et d'hôtel auraient été faciles à documenter, ce d'autant plus que le décompte fourni fait référence à un fichier « LONDON mission expense report.pdf ».

Dans la mesure où la partie civile n'a pas jugé utile de fournir au Tribunal ces informations détaillées dont elle disposait pourtant, et face aux contestations de la défense quant au quantum de la demande, la partie civile n'a – sans être confronté à une quelconque difficulté probatoire – pas fourni la preuve du montant qu'elle allègue.

Ce chef de la demande est dès lors à déclarer non fondé.

ad d). La partie civile n'a pas expliqué à l'audience pour quelle raison elle aurait subi un préjudice spécifique en relation avec le client « **CL1.)** », ni versé aux débats le fichier « CLS Invoice 0970003474.pdf » mentionné dans son décompte.

En l'absence de la moindre preuve, ce chef de la demande est dès lors à déclarer non fondé.

ad e). La partie civile ne verse aucune pièce et ne fournit aucune explication de ce qu'elle entend par « impact interne ».

Le Tribunal étant laissé dans l'ignorance de la nature même du préjudice pour lequel une indemnisation est réclamée, ce chef de la demande est à déclarer non fondé.

Cette conclusion s'impose d'autant plus que le montant de 20.893,60 euros n'est pas un chiffre rond d'estimation mais doit correspondre à des calculs précis, que la demanderesse au civil n'a cependant pas jugé utile de détailler.

ad f). Pour le dernier poste, relatif à une perte de revenus, le montant de 62.680,80 euros semble également correspondre à un calcul précis qui n'a cependant pas été autrement expliqué, ni documenté.

La partie civile n'a fourni aucune indication ni quant aux prestations qu'elle facture ordinairement à ses clients, ni quant à celles qu'elle n'a pas pu facturer en raison de l'incident.

En l'absence de la moindre preuve, ce chef de la demande est dès lors à déclarer non fondé.

La partie civile doit dès lors être déclarée fondée pour le montant de 4.750 + 4.519 = 9.269 euros.

P A R C E S M O T I F S :

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

statuant au pénal

c o n d a m n e X.) du chef des infractions retenues à sa charge à une peine d'emprisonnement de **QUINZE (15) mois** et à une amende de **QUATRE MILLE (4.000)** euros, ainsi qu'aux frais de sa poursuite pénale, ces frais liquidés à 45,42 euros,

f i x e la durée de la contrainte par corps en cas de non-paiement de l'amende à **QUATRE-VINGT** (**80**) jours,

statuant au civil

d o n n e acte à la société anonyme **SOC1.)** S.A. de sa constitution de partie civile,

se **d é c l a r e** compétent pour en connaître,

d é c l a r e la demande recevable en la forme,

d i t la demande civile fondée et justifiée à concurrence de **9.269 euros**,

c o n d a m n e X.) à payer à la société anonyme **SOC1.)** S.A. le montant de **NEUF MILLE DEUX CENT SOIXANTE-NEUF EUROS (9.269 €)**, avec les intérêts légaux à partir du 10 novembre 2011 jusqu'à solde,

c o n d a m n e X.) aux frais de la demande civile dirigée contre lui.

En application des articles 14, 15, 16, 28, 29, 30, 65, 66, 509-1, 509-2 et 509-3 du Code pénal et des articles 2, 3, 155, 179, 182, 183-1, 184 189, 190, 190-1, 194, 195 et 196 du Code d'Instruction Criminelle, dont mention a été faite.

Ainsi fait et jugé par Elisabeth CAPESIUS, vice-présidente, Elisabeth EWERT et Jean-Luc PÜTZ, juges, et prononcé en audience publique le jeudi, 14 juin 2012, au Tribunal d'arrondissement de et à Luxembourg par Elisabeth CAPESIUS, vice-présidente, assistée de Mireille REMESCH, greffière, en présence de Nadine SCHEUREN, substitut du Procureur d'Etat, qui à l'exception de la représentante du Ministère Public, ont signé le présent jugement.