**Scénarios/thèmes pour l’exercice méthodologique**

|  |
| --- |
| **Étude de cas n° 1** Faits/Scénario Bobby est policier. Une nuit, alors qu’il est en service, il aperçoit une Mercedes garée devant chez lui. Il ne reconnaît pas la voiture, mais suppose qu’elle appartient au patron de son épouse. Il téléphone au poste de police et demande à Mary, l’opératrice informatique, de lui dire à qui appartient la Mercedes en expliquant que celle-ci vient de griller un feu rouge. Mary confirme que la voiture appartient bien au patron de sa femme.  *Bobby a-t-il commis une infraction pénale ?*   * **Questions à résoudre**   *Bobby a-t-il accédé de manière illégale à un système informatique ?*   * **Points de discussion**   C’est Mary qui a accédé à l’ordinateur, pas Bobby. Étant autorisée à accéder aux dites données, celle-ci a agi en toute innocence. Par contre, c’est Bobby qui, agissant par l’intermédiaire d’un agent innocent, a provoqué l’accès aux données. Il a menti à Mary (selon un procédé relevant de l’ingénierie sociale). Cela équivaut-il à un accès illégal ?  Bobby et Mary ont tous deux le droit d’accéder à l’ordinateur de la police, mais sous réserve de conditions strictes liées à une demande légitime en rapport avec l’activité de la police. Un accès non conforme à ces conditions constitue-t-il une infraction ?  Que se passerait-il si Bobby se rendait au poste de police et parvenait à regarder par-dessus l’épaule de Mary (« *shoulder surfing* ») pendant que celle-ci effectue une enquête légitime sur la propriété de la Mercedes ?  En regardant par-dessus l’épaule de Mary, Bobby est parvenu à accéder à des données informatiques. On peut s’interroger sur son « intention » et, bien sûr, il n’a pas manipulé le système informatique pour y accéder, mais il a tout de même obtenu un accès délictuel (bien que cela soit très difficile à prouver).  Cette étude de cas est conçue pour amener les délégués à réfléchir à la question de l’autorisation (accès délictuel).  Les délégués pourraient également être invités à réfléchir à la situation dans laquelle se trouverait Bobby s’il se rendait au poste de police et recherchait les informations relatives à la propriété de la Mercedes sur un système à cartes contenant les mêmes informations que celles stockées sur l’ordinateur ? Ce qu’il faut retenir, c’est que ce ne sont pas les données elles-mêmes qui sont protégées (bien qu’elles puissent l’être en vertu d’autres lois sur la protection des données, au regard desquelles la mauvaise conduite de Bobby pourrait également constituer une infraction), mais le support sur lequel lesdites données sont stockées.  Les systèmes informatiques de la police contiennent de grandes quantités d’informations personnelles relatives à des individus, ainsi que nombre d’informations sensibles. L’accès à ces données ne doit être accordé qu’aux personnes ayant un intérêt légitime. Au Royaume-Uni, il est fréquent que des policiers et des opérateurs informatiques de la police accèdent illégalement aux systèmes de leur organisation à des fins personnelles par exemple pour trouver des informations susceptibles d’intéresser la presse ou, dans le cas de policiers corrompus, pour découvrir des informations détenues sur une personne précise ou savoir si un individu ou un groupe donné fait l’objet d’une enquête active. |
| **Étude de cas n° 2**   * **Faits/Scénario**   Un agent de sécurité d’une banque est approché par un groupe de criminels qui lui demande de placer un dispositif — appelé Key Logger et permettant d’enregistrer les frappes de l’utilisateur — à l’arrière d’un certain nombre de terminaux situés dans les locaux de son organisation. Ce Key Logger permet donc de saisir les mots de passe et autres informations qui permettraient à une personne ayant accès à l’un des terminaux en cause de se connecter aux comptes utilisateurs du personnel de la banque.  Une fonction supplémentaire du dispositif Key Logger permet d’enregistrer les appels téléphoniques Skype passés par l’utilisateur du terminal.  Les criminels ont également placé sur le bureau un mouchard qui capte les sons, y compris tous les appels téléphoniques passés et reçus par l’utilisateur du terminal.  *Y a-t-il eu interception illégale ?*   * **Questions à résoudre**   *Y a-t-il eu interception ?*  *Cette interception a-t-elle été réalisée par des moyens techniques ? Des données ont-elles été transmises vers ou depuis un système informatique ?*   * **Points de discussion**   Le Key Logger est un dispositif technique qui capte les données transmises par le terminal. Ce procédé équivaut à une interception clairement illégale.  Qu’en est-il des appels Skype ? Dans ce scénario, il semble que les données circulent sur la même ligne que les autres données transmises par l’ordinateur, mais que se passerait-il si l’utilisateur disposait d’un téléphone Skype autonome ? Un tel téléphone constituerait-il un système informatique ? La Convention de Budapest définit un « système informatique » comme « *tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d’un programme, un traitement automatisé de données* » et les « données informatiques » comme « *toute représentation de faits, d’informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu’un système informatique exécute une fonction* ».  L’utilisation du mouchard audio peut être un peu plus difficile à qualifier. S’agit-il d’une « interception » ? Au Royaume-Uni, les tribunaux ont estimé que pour qu’une interception ait lieu, il doit y avoir une sorte d’interférence ou de soustraction du signal pendant sa transmission sur le réseau. Dans le cas présent, l’enregistrement a lieu indépendamment de la transmission, même si les informations obtenues sont identiques à celles qui l’auraient été si le dispositif avait été placé sur la « ligne ».  Que se passerait-il si le Key Logger était placé sur le système par l’entreprise qui souhaite s’assurer que ses employés n’utilisent pas internet à des fins inappropriées ?  La plupart des systèmes de télécommunications passent à la fois par des réseaux publics et privés. Au moment où la communication quitte vos locaux, elle passe d’un système privé à un système public. Le contrôleur d’un système privé a le droit d’accéder aux communications utilisant ce système ; ainsi, vous seriez en droit de surveiller les conversations sur la ligne téléphonique de votre domicile, à condition que le dispositif technique que vous utilisez pour ce faire soit connecté au côté privé du système.  Ce scénario est conçu pour que les délégués examinent chacun des éléments de l’interception en se posant notamment la question de savoir si cette dernière a permis d’obtenir des données informatiques pendant leur transmission en recourant illégalement à un procédé technique.  Les délégués doivent bien comprendre que cette disposition vise à protéger le contenu des communications plutôt que les informations liées à l’adressage du message ou au coût du service. |
| Étude de cas n° 3   * **Faits/Scénario**   Une organisation criminelle communique à l’aide d’un système de courrier électronique accessible par internet partout dans le monde. Plutôt que de s’envoyer des messages susceptibles d’être interceptés par la police ou qui pourraient les incriminer s’ils étaient trouvés sur leur ordinateur, ces criminels utilisent un système de boîtes aux lettres mortes. Les autres membres de l’organisation possèdent le mot de passe qui leur permet d’accéder au compte de courrier électronique, de lire le message et d’y répondre.  Si la police pouvait accéder à la boîte de brouillons, cela constituerait-il une interception ?   * **Questions à résoudre**   *Le message est-il transmis ?*   * **Points de discussion**   La plupart des États exigent de la police qu’elle nourrisse de forts soupçons avant d’autoriser l’interception du contenu d’une communication. L’obtention de preuves sans l’autorisation requise peut entraîner l’arrêt de l’affaire ou l’irrecevabilité des preuves.  Les ordinateurs et internet facilitent un certain nombre de formes différentes de communication, par exemple le courrier électronique, la messagerie instantanée, Twitter, etc. Les messages sont souvent stockés avant d’être récupérés par leur destinataire. Un message n’ayant pas encore été récupéré doit-il être considéré comme en cours de transmission ? Il n’existe aucun moyen de savoir si le brouillon du message a été lu par le destinataire voulu. La loi devrait-elle accorder la même protection à ceux qui choisissent délibérément de contourner les moyens normaux d’envoi de communications par courrier électronique qu’à ceux qui utilisent ce procédé conformément à sa vocation ?  Il s’agit d’un moyen assez courant pour les criminels de communiquer entre eux. Le fait de chercher à accéder à ces messages — dans le cadre d’une interception ou pas — dépendra du droit interne et/ou de l’attitude des tribunaux nationaux. Cependant, les délégués auraient sans doute avantage à réaliser qu’en cas de recours à l’entraide judiciaire dans le but d’obtenir ces données, l’État requis pourrait considérer qu’il s’agit d’une interception ou, au moins exiger un niveau de soupçon plus élevé de manière à pouvoir obtenir de l’autorité judiciaire compétente l’autorisation d’accéder au contenu de la communication. |
| **Étude de cas n° 4**   * **Faits/Scénario**   Bobby, policier de son état, est entré en possession du téléphone de son épouse, a deviné son mot de passe et a écouté un message vocal enregistré que celle-ci n’avait pas encore récupéré.  *S’agit-il d’une interception ?*   * **Questions à résoudre**   *Le message vocal est-il toujours en cours de transmission ? Y a-t-il eu interception de données informatiques ?*   * **Points de discussion**   Tant que le message n’a pas atteint sa destination, il est probablement encore en cours de transmission, même s’il est stocké dans le système. Le message est vraisemblablement enregistré sous forme numérique sur le serveur de la compagnie de téléphone et Bobby a donc accédé à des données informatiques. Un téléphone est-il un ordinateur ? Probablement oui, puisqu’il effectue un traitement automatisé de données. Les policiers qui effectuent des perquisitions et qui trouvent des téléphones devront peut-être tenir compte de ce point afin de s’assurer qu’ils ont bien l’autorité nécessaire pour accéder à ces messages. La situation serait différente si le destinataire avait écouté le message et choisi de le conserver.  Ce scénario soulève des questions analogues à celles du scénario précédent. Il sert à illustrer ce qui pourrait être une situation assez courante pour des agents qui, dans le cadre d’un mandat de perquisition, saisissent un ordinateur contenant du courrier électronique ouvert et non ouvert. Il sert également à démontrer que l’infraction établie par l’article 3 s’applique à toutes les formes de transfert de données électroniques, que ce soit par téléphone, télécopie, courrier électronique ou transfert de fichiers. |
| **Étude de cas n° 5**   * **Faits/Scénario**   Bobby s’intéresse aux OVNI et pense que le Gouvernement russe a capturé un vaisseau spatial extraterrestre qui aurait atterri en Sibérie au début du XXe siècle. Il visite un site de recrutement militaire russe contenant un lien vers un site exploité par l’armée de l’air russe. L’accès au site nécessite un mot de passe, mais il parvient à y pénétrer à l’aide d’un outil de craquage. Il passe un certain temps à explorer le système et copie plusieurs fichiers. Il essaie également de supprimer tous les fichiers journaux relatifs à son activité afin d’empêcher les Russes de l’identifier. Il modifie ensuite la page d’accueil du site pour qu’elle affiche l’image d’un OVNI à la place de l’insigne de l’armée de l’air.  *Bobby a-t-il commis une infraction ?*   * **Questions à résoudre**   *L’accès non autorisé peut-il constituer en soi une infraction d’atteinte à l’intégrité des données ou du système ?*  *L’effacement de la preuve de l’accès non autorisé constitue-t-il une infraction ?*  *Faut-il que le fonctionnement de l’ordinateur ait été gravement compromis pour que la responsabilité pénale soit engagée ?*   * **Points de discussion**   L’objectif de ces dispositions est de fournir aux données et aux programmes informatiques une protection analogue à celle dont bénéficient les biens corporels contre les dommages intentionnels.  Bobby n’était pas autorisé à accéder au site de l’armée de l’air russe protégé par un mot de passe. Il aurait donc commis une infraction d’accès illégal.  Bobby a supprimé des données, les fichiers journaux et l’insigne de l’armée de l’air. Bien qu’il ait peut-être généré lui-même — de par son activité — les fichiers journaux, ces derniers ne lui appartiennent pas, le système étant configuré pour enregistrer ladite activité. Bobby n’a donc pas le droit de les supprimer. L’armée de l’air a un intérêt légitime à savoir qui accède à son système.  En modifiant l’image de la page d’accueil, il a à la fois supprimé et ajouté des données au système, ce qui, même s’il est peu probable que des informations importantes aient été perdues, risque d’être embarrassant pour l’armée de l’air. Cependant, même si Bobby peut prétendre qu’il a accédé au système uniquement pour supprimer des journaux ou d’autres données sans importance, la question essentielle est de se demander dans quelle mesure un administrateur système peut avoir confiance dans l’intégrité des données après une telle intrusion illégale ?  La réponse à la question de savoir si une infraction a été commise dans ces circonstances relèvera de l’interprétation des autorités locales. Il se peut que le seuil de gravité n’ait pas été établi. Cependant, l’administrateur système se sentira probablement contraint de mettre le site hors ligne afin de déterminer les effets de l’intrusion, s’agissant en particulier d’établir si le site auquel on a eu accès contient des données confidentielles ou sensibles ou s’il est utilisé pour des opérations qui, si elles devaient mal tourner, mettraient en danger le public, s’agissant par exemple d’un système chargé de faire tourner une centrale nucléaire.  Si, pour les besoins de l’argumentation, le système auquel Bobby a accédé était celui utilisé pour faire tourner une centrale nucléaire, les infractions prévues aux articles 4 et 5 seraient-elles suffisantes pour refléter la gravité d’une telle intrusion constituant une attaque contre une infrastructure nationale critique ? |
| **6. Étude de cas n° 6** Faits/Scénario Un programme automatisé de *spam* envoie chaque jour un courriel non sollicité à des milliers d’utilisateurs dans le monde entier. L’ouverture du courriel provoque le téléchargement d’un logiciel sur l’ordinateur de l’utilisateur, lequel n’affecte en rien le fonctionnement de ce dernier. Le logiciel pirate n’acquiert ni ne supprime la moindre donnée stockée et ne provoque pas non plus d’autres dommages. Il a cependant pour effet de transformer l’ordinateur de l’utilisateur en un « zombie » faisant partie d’un « botnet » que le « contrôleur de bot » peut utiliser pour entreprendre divers types d’activités.  *La personne responsable de l’envoi du courriel non sollicité a-t-elle commis une infraction aux articles 4 ou 5 ?*   * **Questions à résoudre**   *Y a-t-il eu accès non autorisé à la machine de l’utilisateur ? Des données ont-elles été modifiées sur la machine de l’utilisateur ?*  *La machine de l’utilisateur a-t-elle été endommagée ?*   * **Points de discussion**   Même si aucun dommage n’a été causé, le logiciel provoque sur l’ordinateur de l’utilisateur une modification des données non autorisée, dans la mesure où l’intéressé n’a reçu aucun avertissement et n’a pas été invité non plus à consentir de quelque manière que ce soit à la modification. L’envoi de courriels non sollicités est-il en soi illégal ou s’agit-il simplement d’une nuisance ? Ne devient-il illégal que lorsqu’il a un impact négatif ?  Que se passe-t-il si le spam contient une pièce jointe et une invitation au destinataire à ouvrir cette dernière du type « Cela devrait vous plaire » ?  On pourrait faire valoir que le destinataire a choisi et donc autorisé le téléchargement de données sur son ordinateur. En réalité, ce consentement n’a pas été donné en toute connaissance de cause, même si d’aucuns font valoir que toute personne choisissant d’ouvrir des pièces jointes provenant de destinataires inconnus le fait à ses propres risques.  Le fait que l’utilisateur ne se soucie pas de savoir si son ordinateur fait partie ou non du « bot net » a-t-il une incidence ? Lorsque nous naviguons sur internet, nous visitons des sites et téléchargeons des données sans tenir compte de la nature du matériel qui peut se retrouver sur notre ordinateur, mais en nous fiant aux noms que les sites web se donnent, aux noms des fichiers ou aux résultats renvoyés par notre moteur de recherche pour nous aider à prendre une décision. Le fait de cliquer sur la vignette d’une image afin d’afficher cette dernière en taille réelle indique que nous sommes conscients des données que nous cherchons à acquérir et que nous avons donné notre consentement en toute connaissance de cause quant à la nature desdites données. Si après avoir cliqué sur une vignette représentant une voiture, nous découvrons que l’image en taille réelle obtenue est celle d’un avion, on ne saurait considérer que nous avons donné notre consentement à l’acquisition de ces données.  Le choix de cliquer sur un lien vers un site web entraîne le téléchargement d’un grand nombre de données. S’il s’agit d’un site licite, la majeure partie de ces données concernera probablement le contenu du site, même si une portion pourra être constituée de publicités placées par des tiers. Là encore, nous avons fait un choix éclairé et donné un consentement implicite pour recevoir la publicité, sachant qu’il s’agit d’une pratique courante sur internet. Une autre pratique courante dans ce secteur consiste à télécharger des données qualifiées de « *cookies* » dans votre navigateur.  Les cookies remplissent diverses fonctions, dont l’enregistrement de l’historique de navigation d’un utilisateur. Ce dernier ayant la possibilité de désactiver la fonction « cookie » de son navigateur, d’aucuns considèrent que cette option suffit à induire qu’il a par la suite donné son consentement au téléchargement desdites données. |
| **7. Étude de cas n° 7**   * **Faits/Scénario**   Bobby est un ancien policier licencié pour utilisation abusive du système informatique de son organisation. Il décide de se venger de la police en recourant à un programme de courrier électronique permettant d’envoyer 70 000 courriels par heure à son ancien service. Il modifie l’en-tête du courriel pour faire croire qu’il provient du chef de la police, trompant ainsi le serveur de courrier électronique de la police en lui faisant croire qu’il provient d’une source légitime. Le serveur de la police n’ayant pas pu gérer un tel afflux, il s’est effondré.  *S’agit-il d’un délit d’ingérence dans le système ?*   * **Questions à résoudre**   *L’envoi d’un courriel implique l’accès ou la tentative d’accès à un système informatique, à savoir le serveur de courrier électronique. Dans quelle mesure le propriétaire d’un tel serveur autorise-t-il cet accès ?*  *Le fait de disposer d’une adresse électronique, ne signifie-t-il pas que vous invitez d’autres personnes à vous envoyer des courriels ?*   * **Points de discussion**   La question est une question de droit. Bobby a accédé à un système dont il a provoqué l’effondrement en y introduisant des données. En créant une adresse électronique accessible au public, le propriétaire de ladite adresse donne implicitement son consentement à la réception de messages. Bobby pourrait faire valoir que la police a consenti à la réception de chaque courriel individuel et qu’il ne saurait être tenu responsable de l’incapacité dudit système à gérer autant de messages. Mais y a-t-il vraiment eu consentement ? Le propriétaire d’une maison donne son consentement implicite au facteur pour que ce dernier insère dans sa boîte aux lettres les lettres qui lui sont adressées. Il consent aussi implicitement à recevoir du courrier « indésirable », comme des prospectus vantant les mérites d’une pizzeria. Le propriétaire ne consent cependant pas à recevoir une telle quantité de prospectus qu’il ne peut même plus ouvrir sa porte d’entrée.  Ne pourrait-on pas également dire qu’en modifiant les coordonnées de l’expéditeur du courriel, l’accès au serveur de courrier électronique a été obtenu par fraude ? Le consentement n’est pas donné pour la réception de tels courriels dits « trompeurs ».  Si ce scénario concerne les courriels, le principe est le même pour ceux qui cherchent à provoquer l’effondrement de sites web en déclenchant une attaque par déni de service, le site étant incapable de gérer le volume de trafic qui lui est destiné. La connexion à un site web implique l’échange de données entre ce dernier et l’ordinateur de l’utilisateur. Des questions analogues concernant le consentement implicite à la connexion au site se posent, comme nous l’avons déjà vu à propos des courriels. |
| **Étude de cas n° 8**   * **Faits/Scénario**   Bobby envoie un courriel à son ex-épouse sur le lieu de travail de celle-ci. Il modifie l’en-tête pour faire croire que le message provient d’un de ses amis. Ledit courriel abrite en fait un programme appelé « Access all areas » qui permet à Bobby de prendre le contrôle de l’ordinateur de son ex. Avant que Bobby n’ait eu la possibilité d’utiliser le programme, sa présence est détectée par l’administrateur système qui arrête le système afin de procéder à une évaluation de l’ampleur de l’intrusion.  *Bobby a-t-il commis une infraction à l’article 5 ?*   * **Questions à résoudre**   *Bobby a-t-il provoqué une suppression de données contenues dans le système ?*  *Bobby a-t-il entravé le fonctionnement d’un système informatique ?*  *Cette suppression de données ou cette entrave au fonctionnement du système était-elle illégale ?*   * **Points de discussion**   La réaction de l’administrateur au courriel de Bobby a eu pour conséquence de priver les utilisateurs du système de tout service. L’accès aux données détenues dans le système a donc été empêché, même si c’est probablement pour une durée limitée. L’infraction n’exige pas que les données soient rendues définitivement indisponibles.  Nous avons discuté de la question de savoir dans quelle mesure le propriétaire d’une adresse électronique consent à recevoir des données de tiers.  L’article 5 concerne les systèmes informatiques, c’est-à-dire un ou plusieurs ordinateurs reliés entre eux. Un ordinateur isolé connecté à internet fait-il partie d’un système ?  L’ordinateur de travail de l’ex-épouse de Bobby fait plus que probablement partie d’un système, dans la mesure où il est vraisemblablement relié à un réseau local (LAN), un réseau étendu (WAN) ou un intranet. Bobby a-t-il entravé le fonctionnement dudit système ?  Bobby pourrait prétendre qu’il n’est pas responsable du déni de service et qu’il n’avait pas l’intention de provoquer un tel événement. Bien au contraire, il voulait que le système continue à fonctionner afin de pouvoir espionner son ex-épouse. Souvent, les attaques par déni de service ne suffisent pas à mettre un site web hors ligne, même si les fournisseurs d’accès internet (FAI) réagissent fréquemment en mettant le site en cause hors service afin de minimiser l’effet de l’attaque sur leurs systèmes et les inconvénients pour les autres clients.  Dans ce scénario, Bobby ne semble pas avoir nourri l’intention requise pour commettre une infraction au titre de l’article 5, ce qui ne signifie pas pour autant qu’il échappe à toute responsabilité pénale.  Il s’agit d’un exemple de Cheval de Troie, à savoir un procédé utilisé couramment par les cybercriminels pour accéder aux ordinateurs d’autrui. |
| **9. Étude de cas n° 9**   * **Faits/Scénario**   Un groupe « hacktiviste » en ligne, hostile à l’utilisation d’animaux pour tester des produits cosmétiques, lance des attaques par déni de service distribué (DDOS) contre les sites web de sociétés fabriquant des produits de beauté et de magazines glamours. Par l’intermédiaire de son propre site web, ledit groupe distribue un logiciel appelé « Supergun » qui lui permet de coordonner les attaques sur les sites visés et de maximiser ainsi le volume de trafic cherchant à accéder aux dits sites à un moment donné. Le logiciel « Supergun » a été développé à l’origine comme un outil permettant aux administrateurs système de tester la sécurité de leurs installations. Cependant, même si le logiciel fonctionne toujours exactement de la même manière, l’interface utilisateur a été rendue beaucoup plus facile à utiliser par le groupe et porte désormais le logo de ce dernier.  *La mise à disposition de Supergun pour téléchargement constitue-t-elle une infraction ? Et sa possession ?*   * **Questions à résoudre**   *Le fait que Supergun puisse être utilisé à des fins légitimes signifie-t-il qu’aucune poursuite ne peut être engagée ?*  *Le fait de mettre Supergun à disposition pour téléchargement équivaut-il à une distribution ?*   * **Points de discussion**   Les infractions visées par cet article sont l’accès non autorisé, l’interception illégale, l’atteinte aux données et aux systèmes.  Si le logiciel était à l’origine à double usage, c’est-à-dire qu’il remplissait une fonction légitime, le fait que l’interface utilisateur ait été modifiée signifie-t-il que sa possession constitue désormais une infraction ?  Si l’on se réfère à nos études de cas précédentes, le logiciel « Access all areas » utilisé par Bobby pour accéder à l’ordinateur de son ex-épouse a une fonction légitime. Des programmes comme celui-ci permettent en effet aux utilisateurs d’accéder à distance à leur propre ordinateur. Qu’en est-il de la possession par Bobby d’un logiciel de craquage de mots de passe ? C’est peut-être une question d’intention. En d’autres termes, a-t-il une raison légitime de posséder un tel logiciel ? Existe-t-il des preuves montrant qu’il a cherché à déployer ce logiciel dans le but de commettre une infraction ?  Cette infraction n’est pas destinée à sanctionner les fournisseurs et utilisateurs légitimes de logiciels. Lorsque, comme c’est le cas en l’occurrence, il existe des preuves d’une intention malveillante, le problème ne se pose peut-être pas. Cependant, les personnes pratiquant la cybercriminalité mènent souvent aussi des activités légitimes sur internet et peuvent être des professionnels du secteur qui utilisent et développent ces logiciels, quitte à les mettre au service d’une activité illégale lorsque l’occasion s’en présente. Qu’en est-il des magasins vendant des logiciels ou du matériel ? Comment sont-ils censés savoir quelles sont les intentions d’un client par rapport à un matériel ou un logiciel particulier ? La portée de l’infraction est-elle trop vague ? |
| **Étude de cas n° 10**   * **Faits/Scénario**   Un éditeur de logiciels a développé un logiciel de cryptage qui divise le contenu du disque dur en deux volumes protégés chacun par un mot de passe différent. Cependant, seul un volume est visible à l’utilisateur ordinaire et l’existence du volume caché ne peut pas être détectée à l’aide des logiciels d’expertise judiciaire en informatique actuellement disponibles.  Selon les développeurs, ce logiciel serait utile à toute personne contrainte de révéler son mot de passe. En d’autres termes, les données stockées sur le volume caché peuvent être conservées en toute sécurité, même en cas de divulgation du mot de passe protégeant le dossier visible.   * **Questions à résoudre**   *Le développement, la production, la distribution, l’utilisation ou la possession d’un tel logiciel constituent-ils une infraction pénale ?*   * **Points de discussion**   Nous sommes tous constamment invités à sécuriser nos données. Si un tel programme peut manifestement s’avérer utile aux individus se livrant à des activités criminelles, et en particulier à celles qui craignent que le contenu de leur ordinateur ne les incrimine, les intéressés ne l’utilisent pas pour commettre une infraction, mais plutôt pour dissimuler des preuves.  Les cybercriminels peuvent utiliser d’autres programmes ou systèmes pour éviter d’être repérés, notamment des programmes d’anonymisation qui leur permettent de surfer sur internet sans divulguer leur véritable adresse IP ou des programmes d’élimination des preuves capables d’effacer le contenu d’un disque dur. |
| **Étude de cas n° 11**   * **Faits/Scénario**   Nick travaille au service informatique d’une grande entreprise qui possède son propre intranet. La politique de l’entreprise interdit à ses employés d’utiliser l’ordinateur et la connexion internet de leur entreprise pour effectuer des achats en ligne. Pendant son temps libre, Nick commence à développer un logiciel qui permettrait à l’entreprise d’identifier les employés effectuant des paiements en ligne et de saisir ces informations afin qu’elles puissent être utilisées comme preuves dans le cadre de procédures disciplinaires. Nick n’ayant pas les compétences nécessaires, il prend contact en ligne avec « Jupiter ». Ensemble, ils développent un logiciel qui, une fois téléchargé sur l’ordinateur d’un utilisateur, s’active lorsque ce dernier commence à remplir un formulaire électronique, tel que celui utilisé pour traiter les paiements en ligne, et capture les données saisies. L’entreprise de Nick est très satisfaite tandis que Jupiter commence à déployer le logiciel à l’aide d’un Cheval de Troie.  *Nick a-t-il commis une infraction ?*  *L’entreprise a-t-elle commis une infraction ?*  *Jupiter a-t-il commis une infraction ?*   * **Questions à résoudre**   *L’appareil a-t-il été conçu ou adapté principalement dans le but de commettre les infractions pénales susmentionnées ?*   * **Points de discussion**   Les cybercriminels ont accès à une variété d’outils qui leur permettent de commettre des infractions ou les y aident. Il est ainsi possible d’acheter le code qui vous permettra de construire votre propre « bot » ou d’acheter un « bot net » ou encore d’acheter l’accès à un bot net qui permettra à l’utilisateur de commettre divers types de délits tels que « l’hameçonnage » (*phishing*).  Jupiter utilise ce programme pour obtenir des utilisateurs des informations financières qu’il pourra exploiter lui-même ou dont il pourra confier le traitement à des tiers. Cette société a sans doute supposé que Nick avait produit le programme dans le cadre de son travail. Nick est innocent et a aidé par inadvertance Jupiter à se doter d’un puissant outil potentiellement utilisable à des fins criminelles. Ni Nick ni sa société n’ont l’intention criminelle requise. La situation serait-elle différente si Jupiter continuait à commercialiser le programme auprès d’autres entreprises qui souhaitent surveiller l’activité internet de leurs employés ? Jupiter pourrait-elle faire valoir que le logiciel a un but légitime malgré son attrait évident aux yeux des criminels ? |
| **Étude de cas n° 12**   * **Faits/Scénario**   Stefan utilise un logiciel de photographie disponible dans le commerce pour produire une traite bancaire réaliste sur son ordinateur personnel. Il présente la traite à sa banque qui l’accepte comme authentique et transfère les fonds sur le compte de Stefan.  *Quelle infraction Stefan a-t-il commise ?*   * **Questions à résoudre**   *La production de la fausse traite bancaire s’analyse-t-elle en une infraction de faux et usage de faux (falsification) ?*  *L’infraction n’est-elle complète qu’une fois la traite acceptée comme authentique par l’employé de banque ?*   * **Points de discussion**   La création de la traite bancaire implique la saisie de données non authentiques dans un ordinateur, à savoir que la traite a été établie en faveur de Stefan. Cependant, cette opération a-t-elle été effectuée de manière illégitime ou Stefan a-t-il le droit de produire un tel document sur son propre ordinateur ? Stefan pourrait avoir eu l’intention d’utiliser la traite pour escroquer la banque, mais, pour une raison quelconque, n’être jamais passé à l’acte. Le fait que ce document soit un jour produit sur papier fait-il une différence au niveau de l’engagement de la responsabilité de Stefan ?  Cette infraction n’a pas vraiment été créée pour traiter ce type de scénarios, bien qu’elle puisse servir si la législation nationale ne criminalise pas autrement la production d’une fausse traite bancaire. Elle relève d’un type d’infractions qu’il convient mieux de traiter sous l’angle de la responsabilité secondaire (tentative par exemple).  Cette infraction vise en réalité les personnes utilisant un ordinateur comme moyen de commettre leurs agissements. Ainsi, lorsqu’il agit de bonne foi, l’employé de banque saisit les données fournies par Stefan en supposant que celles-ci sont authentiques. |
| **Étude de cas n° 13**   * **Faits/Scénario**   Au cours de son adolescence, Stefan s’est toujours vanté auprès de ses amis de ses prouesses sportives. Ses amis sont sceptiques. Il parvient à accéder à la base de données de son ancienne école et modifie son dossier pour prouver qu’il était capitaine de l’équipe d’athlétisme de l’établissement et qu’il a remporté un certain nombre de médailles.  *S’agit-il d’une infraction de falsification informatique ?*   * **Questions à résoudre**   *Les données qui ont été modifiées ne seront pas utilisées à des fins légales*.   * **Points de discussion**   Stefan a modifié des données et introduit des données non authentiques. Il est clair que cet accès et cette altération sont illégaux. Abstraction faite des autres infractions que Stefan pourrait avoir commises, il est douteux qu’il se soit livré à une falsification informatique, car les données en cause ne seront pas utilisées à des fins légales.  L’infraction de falsification n’est pas liée à un gain financier ou autre ; ce type d’infractions relève en effet de la fraude informatique. Cet article vise à assurer la sécurité et la fiabilité des données électroniques pouvant avoir des conséquences sur les relations juridiques. L’expression « à des fins juridiques » fait référence aux transactions et aux documents juridiquement pertinents. |
| **Étude de cas n° 14**   * **Faits/Scénario**   Maintenant qu’il a perdu son emploi dans la police et qu’il doit verser une pension alimentaire à son épouse à la suite de leur divorce, Bobby cherche un autre moyen de gagner de l’argent. Il a toujours été intéressé par le négoce de valeurs mobilières et achète 1 000 actions de Flanders Mining Inc, une société ayant le droit exclusif d’extraire de l’uranium en Belgique, pour 1 EUR pièce. Bobby est membre d’un forum internet dont les participants sont, comme lui, intéressés par le marché boursier. Bobby poste un message disant qu’un de ses amis au sein du Gouvernement belge lui aurait confié la découverte de quantités substantielles d’uranium en Belgique. Cette annonce fait décoller le cours de l’action de Flanders Mining qui, à la fin de la semaine, atteint 1 000 EUR. Bobby vend alors ses parts.  *Bobby a-t-il commis une infraction ?*   * **Questions à résoudre**   *Le message de Bobby est-il faux ?*  *Si le message est faux, une autre personne a-t-elle perdu un bien en conséquence ? Bobby a-t-il retiré un avantage économique ?*   * **Points de discussion**   Si le message posté par Bobby est faux, il peut avoir commis une infraction. Il a introduit de fausses données dans un ordinateur et a tiré un avantage économique de la hausse du cours de l’action.  Le lien de causalité entre la saisie des données et l’effet produit est-il faible ?  Bobby a-t-il causé une perte à une autre personne ? On peut soutenir que oui, dans la mesure où les actions sont mal évaluées et vont probablement baisser à un moment donné. Cependant, force est de reconnaître que le marché des actions est extrêmement volatil.  La valeur d’une action n’est-elle pas le prix que quelqu’un est prêt à payer pour l’acquérir à un moment donné ? Quelqu’un a-t-il vraiment été escroqué, ce type de rumeurs et de messages n’est-il pas répandu sur internet ? Quelqu’un va-t-il vraiment croire ce message et refuser d’y voir une tentative maladroite de manipuler le prix de l’action ? Cela signifie-t-il que nous ne pouvons pas proférer de mensonges sur internet ? |
| **Étude de cas n° 15**   * **Faits/Scénario**   Stefan se rend en voiture à la banque. Sur le parking, il constate qu’il n’a pas assez de monnaie. Il met une rondelle dans le parcmètre et obtient un ticket.  *Stefan a-t-il commis une infraction ?*   * **Questions à résoudre**   *L’horodateur est-il un ordinateur ?*  *Est-il important que le parcmètre produise des tickets automatiquement et qu’aucun être humain n’ait été trompé ?*  *Quel est le statut du ticket de stationnement ?*   * **Points de discussion**   L’horodateur est un ordinateur, il traite les données, calcule la somme d’argent déposée et, sur la base du tarif de stationnement, émet un ticket pour la durée appropriée. Stefan a introduit des données non authentiques, à savoir la rondelle plutôt que la pièce appropriée. L’article 7 n’exige pas qu’un être humain ait agi sur les données fournies.  Le ticket de parking est un faux, les données utilisées pour le créer étaient fausses et il a été produit afin qu’une personne, en l’occurrence le gardien du parking, le considère comme authentique et ne verbalise pas Stefan pour défaut de titre de stationnement. |
| **Étude de cas n° 16**   * **Faits/Scénario**   Après son arrestation, la police découvre que Stefan est en possession des données de cartes de crédit d’un grand nombre de tiers.  *La possession de ces données constitue-t-elle une infraction pénale ?*   * **Questions à résoudre**   Quel est le statut des fichiers informatiques ? Sont-ils des « choses » en droit bien qu’ils se composent uniquement d’une chaîne de code binaire ?   * **Points de discussion**   Au Royaume-Uni, la possession d’un article destiné à être utilisé dans le cadre d’une fraude constitue une infraction de droit pénal matériel. La notion d’article englobe un fichier informatique. Il faut bien sûr prouver l’intention nécessaire, mais il paraît difficile de faire valoir une raison légitime d’être en possession de données de ce type.  Il se pourrait que cette détention soit considérée comme une infraction préparatoire. |
| **Étude de cas n° 17**   * **Faits/Scénario**   Adam est membre d’un groupe en ligne très fermé qui échange des photographies d’enfants victimes d’abus sexuels. Adam est également membre d’un réseau de partage de fichiers « Peer to Peer » [entre homologues]. Il place les photos d’enfants victimes d’abus sexuels qu’il a obtenues du groupe en ligne dans des dossiers partagés en Peer to Peer, ce qui les rend accessibles aux autres membres du réseau.  *Quelles infractions Adam a-t-il commises ?*   * **Questions à résoudre**   *Définitions de la production, de l’obtention et de la distribution.*  Adam a téléchargé des fichiers d’images depuis internet. Le téléchargement équivaut-il à la production de telles images ? Télécharger un fichier, et en particulier l’enregistrement d’une image sur un ordinateur, ne saurait être assimilé à regarder passivement la télévision. L’acte de téléchargement crée une nouvelle chose, à savoir un fichier informatique. Ainsi, la visualisation d’images sur internet implique la création de nouvelles images. Les procureurs pourraient trouver ce concept utile.  Les réseaux de partage de fichiers Peer to Peer permettent aux membres d’accéder aux fichiers mis à leur disposition par d’autres membres. En plaçant les images dans le dossier partagé, Adam les rend disponibles à la diffusion. |
| **Étude de cas n° 18**   * **Faits/Scénario**   Bill est arrêté à l’aéroport à son retour du Cambodge. On découvre que son ordinateur portable renferme un grand nombre d’images le montrant en train de se livrer à des activités sexuelles avec des enfants qui semblent originaires d’Asie du Sud-Est.  *Bill peut-il être poursuivi au titre de la production ou de la possession de ces images ?*   * **Questions à résoudre**   *Compétence.*  *Choix de l’infraction matérielle : possession des images ou production des images.*   * **Points de discussion**   La production des images pourrait soulever des problèmes de compétence, car elles semblent avoir été réalisées à l’étranger.  La possession ne devrait pas être un problème. |
| **Étude de cas n° 19**   * **Faits/Scénario**   WWW.Iuvfishin.com est un site web consacré à la pêche et hébergé sur des serveurs situés aux États-Unis. Les propriétaires du site découvrent qu’il a été piraté et qu’un millier d’images de pédophilie ont été téléchargées et intégrées dedans. En raison du mode opératoire, lesdites images ne sont pas visibles pour les utilisateurs ordinaires du site. Le site enregistre les adresses IP des personnes ayant accédé aux photographies.  Une adresse IP attribuée à John a été communiquée à la police de votre pays. Celle-ci retrouve le domicile de l’intéressé et saisit son ordinateur qui contient des milliers d’images de pédophilie. Il ressort clairement de l’historique du navigateur et des données contenues dans ces fichiers que la plupart des images ont été téléchargées depuis internet.   * **Questions à résoudre**   *Comment prouver que John est responsable de ces images ? Quel est l’impact des poursuites éventuelles sur les suspects accusés d’infractions de pédophilie.*   * **Points de discussion**   Cette méthode de dissimulation des images n’est pas rare. Les groupes affichent des liens vers les images. Cependant, il peut être dangereux de se baser uniquement sur l’adresse IP pour obtenir un mandat de perquisition sans comprendre comment ladite adresse s’est retrouvée connectée au site. Le propriétaire de l’adresse en cause pourrait en effet s’être retrouvé là tout à fait innocemment à la suite de l’activation d’un lien sur un autre site et ne pas avoir accédé aux images après avoir réalisé en quoi elles consistent. Bien entendu, il pourrait également avoir visité le site à plusieurs reprises ou avoir accédé à un certain nombre d’images.  Vous pourriez utiliser cette information pour discuter des précautions à prendre avant d’accuser un individu de pédophilie. Il existe en effet un taux élevé de suicide parmi les personnes soupçonnées de cette infraction. Comme dans toutes les affaires de cybercriminalité, vous devez être en mesure d’identifier avec certitude la personne au clavier au moment des faits. Une adresse IP peut en effet être utilisée par plusieurs personnes ou le réseau sans fil peut avoir été détourné par quelqu’un d’autre. Les accusations de ce type peuvent avoir un effet dévastateur sur une personne innocente. |
| **Étude de cas n° 20**   * **Faits/Scénario**   La police des États-Unis a mis hors service un site web hébergeant des images de pédophilie destinées à des personnes acquittant un abonnement mensuel. Les autorités américaines ont saisi les données des abonnés payants, notamment l’adresse IP, les numéros de carte de crédit, l’adresse électronique, l’adresse de facturation et le mot de passe. L’un de ces clients est Oswald. La police ayant obtenu un mandat de perquisition du domicile de l’intéressé, son ordinateur est examiné. Aucun élément compromettant n’a été trouvé, Oswald ayant eu recours à un programme appelé « Elimination of Evidence » [élimination des preuves].  *Oswald a-t-il commis une infraction ?*   * **Questions à résoudre**   *Oswald a-t-il commis* *une infraction relevant du droit matériel ou une infraction de nature à engager sa responsabilité secondaire ? La compétence juridictionnelle pose-t-elle problème ?*  *Le fait que le site web américain était entièrement automatisé joue-t-il un rôle ?*  *Que dire de l’utilisation du programme d’élimination des preuves ?*   * **Points de discussion**   Oswald n’est en possession d’aucune image et nous ne pouvons pas prouver qu’il a accédé à un site web pour visualiser de telles images, même si nous pouvons établir qu’il a souscrit un abonnement qui lui aurait permis de le faire. Cependant, Oswald a versé de l’argent afin de persuader une autre personne, le propriétaire du site web aux États-Unis, de diffuser ou de mettre à disposition des images à caractère pédophile à des fins de diffusion. Pareil comportement peut-il s’analyser en une infraction pénale ?  Le fait que le site web américain soit entièrement automatisé signifie qu’aucun être humain n’est réellement impliqué dans le traitement des données de la carte de crédit. Pourtant, le processus a été créé par une personne qui en tire un profit financier, qui l’administre et qui en assure la maintenance.  L’utilisation d’un programme d’élimination des preuves n’est pas, en soi, illégale. À moins qu’Oswald n’ait pu activer le programme au cours de l’enquête de police, il est peu probable qu’il ait commis une infraction liée à l’entrave à la justice. Toutefois, si Oswald était poursuivi en justice, le recours à un tel programme pourrait être considéré comme une circonstance aggravante par le tribunal. |