CORRIGE

Ces éléments de correction n'ont qu'une valeur indicative. Ils ne peuvent en aucun cas engager la responsabilité des autorités académiques, chaque jury est souverain.

BREVET DE TECHNICIEN SUPÉRIEUR
INFORMATIQUE DE GESTION

SESSION 2011

CORRIGÉ

ÉPREUVE E3 : ÉCONOMIE – DROIT

Épreuve commune aux deux options

Durée : 4 heures **coefficient : 3**

CALCULATRICE NON AUTORISÉE POUR CETTE ÉPREUVE

Le corrigé comporte 8 pages, numérotées de la page 1/8 à 8/8.

PREMIÈRE PARTIE : TRAVAIL MÉTHODOLOGIQUE *(12 points)*

1. Étude d'une documentation économique *(8 points)*

Analyser les enjeux du recours au service hébergé (ou *cloud-computing*) pour l'entreprise cliente.

Référentiel d'économie d'entreprise
« 4. L'entreprise et sa démarche stratégique
4.3. Les options stratégiques : les stratégies d'impartition »

Nos sociétés sont marquées par une succession d'innovations liées aux technologies de l'information et de la communication (TIC). Après la démocratisation de l'informatique et de l'internet, le développement des techniques de programmation et le développement des réseaux, nous voici à l'aube du « cloud computing » ou de l'« informatique en nuages ».
Avec le cloud computing les applications ou les données ne sont plus présentes localement. Elles sont situées sur un ou plusieurs « nuages » et les entreprises accèdent à la demande à des services sans avoir à gérer d'infrastructure et sans être les propriétaires des ressources. L'accès aux données et aux applications peut se faire à partir de n'importe quel périphérique connecté, le plus souvent au moyen d'un simple navigateur Internet.

La documentation, extraite de la revue « Chef d'entreprise » et « 01 Informatique » de septembre 2010, présente le cloud computing.
Le « cloud computing » désigne ainsi une nouvelle façon d'appréhender l'informatique dématérialisée déclinée sous diverses formes de services « en nuages ». Cette technique représente une rupture technologique et stratégique qui redéfinit complètement le rapport entre les clients et les fournisseurs des produits et services rattachés aux TIC, avec des avantages mais aussi des risques susceptibles d'affecter profondément les entreprises.

Les avantages attendus

- Un recentrage sur le cœur de métier : le cloud computing permet aux entreprises de développer une stratégie de recentrage sur leur métier principal.

- Une mise en œuvre rapide de la solution choisie : le cloud computing est une solution informatique relativement simple à mettre en œuvre pour une entreprise de taille modeste ou une start-up.

- Une réduction des coûts : installation de client léger virtuel et baisse des coûts fixes. Le cloud computing permet, sans investissement majeur en termes d'infrastructures, de bénéficier d'un service à moindre coût. Il permet également une rationalisation de l'utilisation des ressources humaines.

- Une évolution du système d'information facilitée : plusieurs solutions sont envisageables et permettent une certaine évolution de la structure du système d'information. Il est possible de tester un outil avant de le déployer. Les services fournis dans le cadre du cloud computing sont vastes et concernent la capacité de traitement de l'information, les infrastructures informatiques, les capacités de stockage et d'archivage, mais aussi les applications

informatiques. L'offre cloud s'étend à de nouveaux domaines : la finance, la santé, le transport, la distribution.

- Le métier de DSI se transforme. L'approche métier prend le pas sur l'approche technologique et permet une meilleure visibilité des compétences nécessaires à l'entreprise et s'inscrit dans une vision prospective.

Le cloud computing revêt des avantages indéniables pour l'entreprise, en particulier pour les petites structures, qui peuvent ainsi accéder à des services dont elles ne pourraient pas bénéficier dans un autre contexte. Toutefois, cette technique comporte des risques.

Les risques

- Les risques matériels
  - Risque lié à l'indisponibilité du service : avoir la garantie d'une connexion internet et un niveau de bande passante suffisant pour que le fonctionnement des services donne entière satisfaction et ne pénalise pas l'entreprise, doit être le minimum exigé par l'entreprise envers son prestataire.
  - Risque lié à l'interopérabilité avec l'existant : les solutions du cloud sont flexibles et standardisées mais ne permettent pas nécessairement l'interopérabilité avec les solutions propriétaires des entreprises (l'existant).
  - Risque lié aux performances des applications : le niveau de performance peut être décevant et insuffisant pour l'entreprise utilisatrice. Cela dépend du contrat d'origine (précisions des obligations des parties) et suppose des clauses de révision pour éviter les désagréments.

- Les risques liés à la sécurité

La fiabilité du cloud et de son fournisseur en termes de sécurité constitue « le principal frein au déploiement du cloud ».

  - Le recours à ce type de service élargit le périmètre à protéger et rend la tâche de sécurisation du système d'information plus complexe à réaliser. Les failles liées à la mutualisation des ressources sont réelles et obligent les interfaces avec le prestataire à être suffisamment sécurisées. Les risques d'intrusion malveillante sont également très présents dans les critères de décision des entreprises.
  - Le risque de défaillance ou la disparition du prestataire (pérennité du fournisseur) doit être mesuré pour éviter d'en subir les conséquences au niveau de l'entreprise.
  - Le risque de pertes des données est à prendre en considération par l'entreprise utilisatrice.

- Les risques « politiques » ou géographiques

Cela pose le problème de la récupération de données selon le lieu de stockage. Les entreprises ont intérêt à rechercher auprès de leur prestataire une garantie de stockage des données sur des serveurs de proximité. Cela leur permet de ne pas être soumises à un cadre juridique autre que celui du territoire national ou encore de courir le risque d'être inscrites sur une liste noire (« blacklist ») pour des raisons politiques (exemple de la filiale chinoise) et ne plus pouvoir accéder à leurs ressources informatiques.

2. Étude d'une documentation économique *(4 points)*

Montrez que les pays d'Afrique connaissent des inégalités dans leur développement.

Référentiel d'économie générale
« 5. L'hétérogénéité de l'économie mondiale »

Avec presque un milliard d'habitants, le continent africain enregistre depuis une dizaine d'années des résultats supérieurs à ceux de la croissance mondiale. La croissance se définit comme l'augmentation soutenue d'un indicateur de dimension comme le PIB (produit intérieur brut). Lorsque la croissance se traduit par des transformations économiques, sociales et structurelles, on parle de développement, mesuré par l'IDH (indicateur de développement évaluant le niveau de vie, le niveau d'éducation, la longévité).
Le développement des pays d'Afrique est cependant contrasté entre l'émergence de certains pays et les difficultés de certains autres.

1. Les « Lions africains » présentent les caractéristiques des pays émergents (Brésil, Russie, Inde, Chine)

- Les Lions africains sont les locomotives économiques du continent. On peut citer notamment l'Afrique du Sud, l'Égypte, le Maroc, l'Algérie, ou encore le Botswana ou la Libye.
- Ces pays sont caractérisés par un fort taux de croissance économique. À eux seuls, les « Lions » représentent 70% du PIB du continent grâce à :
  - une relative stabilité politique, rassurante pour les investisseurs étrangers,
  - des politiques publiques encourageant l'investissement privé,
  - une ouverture au commerce international par l'exportation de matières premières et d'énergie bénéficiant de la hausse des cours.
- Ces pays connaissent par ailleurs un développement humain en progrès : IDH compris entre 0.68 et 0.77 (exemple : Tunisie, Algérie, Guinée Équatoriale, Botswana, Afrique du Sud).
  - L'espérance de vie s'allonge grâce aux progrès sanitaires et peut atteindre plus de 70 ans dans certains pays comme la Tunisie et l'Algérie.
  - Le taux d'alphabétisation des adultes est assez élevé (peut aller jusqu'à 88% en Afrique du Sud).
  - Le PIB par habitant est désormais supérieur à 7500 US $ en PPA et atteint même 30 000 US $ en PPA pour la Guinée Équatoriale.

2. Cependant la majorité des pays africains demeure des Pays Moins Avancés (PMA)

- Une minorité de pays, les Lions, concentrent à eux seuls 70% du PIB du continent alors que les autres pays africains ne réalisent que 30% du PIB. Cette inégale répartition témoigne de la pauvreté de la majorité des pays du continent. Ces pays sont des PMA.
- Ils se caractérisent par :
  - Une faiblesse des revenus : un PIB par habitant inférieur à 1200 US $ en PPA,
  - Un IDH faible, compris entre 0.34 et 0.39 (exemple : Niger, Sierra Leone, République Centrafricaine, Mali, Burkina Faso) qui révèle un retard du développement du capital humain.
  - Le niveau insuffisant d'éducation et de formation (taux d'alphabétisation des adultes qui descend à moins de 30 %) pèse sur la productivité du travail.

Ainsi, il existe une grande hétérogénéité de développement des pays africains. Seuls les Lions connaissent un développement, tant quantitatif que qualitatif. Ils sont les moteurs du développement du continent.

DEUXIÈME PARTIE : DÉVELOPPEMENT STRUCTURÉ – *(8 points)*

Le droit apporte-t-il une réponse suffisante à la fraude informatique des systèmes d'information ?

Référentiel de droit

« 3. Le cadre juridique de l'activité informatique

3.3 La lutte contre la fraude informatique »

INTRODUCTION *(2 points)*

- Intérêt du sujet : *(0,5 point)*

Les entreprises sont, selon les statistiques, assez vulnérables aux attaques informatiques qui menacent leurs systèmes et leurs données.

« Plusieurs raisons expliquent le développement de la cybercriminalité. La numérisation facilite l'accès aux données. L'utilisation des technologies est un phénomène culturel qui concerne chacun de nous quotidiennement. Elle facilite de surcroît les actes de malveillance ».

Cyberdroit, Le droit à l'épreuve de l'internet – Christiane Féral-Schuhl- Dalloz 5ème édition 2010.

- Définitions : *(0,5 point)*

- Le droit est un corpus de règles qui organise la vie en société.
- La fraude informatique est un « délit commis en utilisant les moyens informatiques. Les principales fraudes sont l'accès par effraction à un système informatique non autorisé, l'usurpation d'identité pour accéder à des ressources ou effectuer des transaction financières ou commerciales, les infractions à la protection de données nominatives [...] ».
  Informatique, Internet et nouvelles technologies de l'information et de la communication – Jacques Gualino – Gualino éditeur 2005.
- Le système d'information regroupe l'ensemble des informations et des moyens matériels et logiciels de traitement associés participant au fonctionnement d'une entreprise.
  Informatique, Internet et nouvelles technologies de l'information et de la communication – Jacques Gualino – Gualino éditeur 2005.

- Problématique : *(0,5 point)*

La réponse du législateur est-elle adaptée aux évolutions rapides de la fraude informatique ?

La problématique étant fortement suggérée dans l'énoncé du sujet, le candidat est amené à la reformuler lorsqu'il précise l'objet de son étude.

Annonce du plan : *(0,5 point)*

Exemple de plan
1ère partie : La Loi Godfrain apporte une réponse adaptée à la fraude informatique
2ème partie : L'apparition de nouvelles formes de fraude informatique conduit le droit à s'adapter

Quel que soit le plan choisi, en deux ou trois parties, le développement doit faire apparaître une opposition (de type oui/non) et/ou une complémentarité (de type oui/mais).
Le développement doit correspondre au plan annoncé.
La recherche de tous les aspects de la problématique n'est pas exigée.
Accepter tout autre plan en deux ou trois parties répondant à la problématique posée par le candidat.

DÉVELOPPEMENT *(5,5 points)*

Les éléments qui suivent seront particulièrement évalués (bien qu'ils puissent ne pas être tous présents).

1ère partie : La loi Godfrain apporte une réponse adaptée à la fraude informatique

La fraude informatique cible essentiellement les entreprises et notamment celles dont les systèmes d'information sont vulnérables à des attaques variées et dont les conséquences peuvent être lourdes. Ceci a suscité une législation dont l'objet est la répression de la fraude informatique, c'est-à-dire l'atteinte aux systèmes d'information et aux données.

❖ Les conséquences de la fraude informatique

La fraude génère des conséquences multiples pour l'entreprise : financières, économiques, organisationnelles et judiciaires.

- La fraude occasionne des conséquences financières considérables pour réparer les dommages matériels causés par les fraudes (restauration des systèmes après un virus ou un vers, perte d'exploitation, renouvellement du matériel),
- La fraude entache l'image de marque de l'entreprise parce qu'elle crée une insécurité (retards dans les réponses aux clients, responsabilité vis-à-vis des clients concernés par les pertes ou l'exploitation des données, etc.),
- La fraude peut porter atteinte à l'intégrité des informations (altérations, falsifications des documents),
- Les fraudeurs peuvent mettre à mal la confidentialité des informations des entreprises,
- L'auteur de la fraude est responsable vis-à-vis des clients concernés par la perte ou l'altération des données (conflit judiciaire possible).

❖ Le cadre juridique depuis 1988 : la loi Godfrain

La loi Godfrain de 1988 a introduit un corpus de règles visant à réprimer les atteintes aux systèmes de traitement automatisé de données. Sont donc concernés tous les systèmes mettant en œuvre simultanément un matériel et un logiciel.

La loi répertorie les infractions suivantes :

- intrusion illégale dans un ordinateur : le délit est constitué par la présence indue dans le système même en l'absence de préjudice,
- sabotage, entraves du système de traitement : le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni (destruction de fichiers, de programmes, de sauvegardes, saturation, introduction de virus ou bombe logique, etc.),
- altération de fichiers et altération des données : introduire frauduleusement des données dans un système de traitement automatisé ou supprimer ou modifier frauduleusement les données qu'il contient est un délit,
- la participation à un groupe de fraudeurs : le groupement formé de fraudeurs en vue de la préparation d'une infraction est un délit,
- la tentative d'infraction est punie des mêmes peines que l'infraction elle-même.

La loi sanctionne les personnes physiques par des peines d'amende et de prison.
Les personnes morales voient leurs sanctions multipliées par cinq (loi sur la responsabilité des personnes morales du 1er mars 1994).
Les personnes physiques et morales peuvent également être sanctionnées par des peines complémentaires (exclusion des marchés publics, publication du jugement, privation des droits civiques, civils et familiaux, etc.).

2ème partie : L'apparition de nouvelles formes de fraude informatique conduit le droit à s'adapter

En plus des activités criminelles traditionnelles, l'internet et l'informatique en réseau ont fait naître une multitude d'infractions nouvelles : captation, diffusion de données personnelles, détournement de systèmes de paiement, fourniture d'outils destinés à commettre des infractions, etc.

❖ Vers une plus grande protection des données et des transactions

- Protection des données

La fraude informatique peut aussi conduire à des atteintes aux droits des personnes du fait des traitements informatiques : collecte frauduleuse de données par hameçonnage ; enregistrement illégal de données (religieuses, raciales…) ; détournement des informations de leur finalité, etc. Les responsables des traitements ont l'obligation de déclarer, de conserver et surtout de sécuriser ces données conformément à la loi.

La loi Informatique, fichiers et libertés de 1978 modifiée en 2004 définit les données à caractère personnel comme « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ».
Exemples : nom, numéro d'identification, voix, image et empreintes digitales.

La sécurité doit se concevoir pour l'ensemble des processus relatifs à ces données, qu'il s'agisse de leur création, leur utilisation, leur sauvegarde, leur archivage ou leur destruction. Elle concerne leur confidentialité, leur intégrité, leur authenticité et leur disponibilité.

- Protection des transactions numériques

Le commerce électronique ne peut se développer sans que soit assurée la sécurité du réseau lui-même. Un rapport de la Commission européenne du 22 avril 2008 fait état d'une augmentation des fraudes aux moyens de paiement. La loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) prend en compte la cryptologie destinée à protéger les données. La mauvaise utilisation des moyens de cryptologie est de nature à engager la responsabilité civile et pénale des auteurs de l'infraction.

❖ **Vers une amélioration en matière de sécurité des systèmes d'information**

L'objectif du législateur étant d'adapter la législation à ces nouvelles situations de fraude, des changements sont indispensables, surtout lorsque l'on sait qu'en matière pénale le principe est celui de l'interprétation stricte et qu'en conséquence le juge ne saurait raisonner par analogie.

Les SI sont aujourd'hui mieux protégés :

- par un renforcement des sanctions avec aggravation des amendes et des peines de prison,
- par un changement de terminologie : la saisie des données par les autorités judiciaires suffit à constater l'infraction (le support matériel n'est plus nécessaire pour constater l'infraction),
- par l'introduction d'une nouvelle infraction qui a vocation à sanctionner la fourniture d'outils destinés à faciliter l'infraction ; il s'agit de sanctionner la fourniture de logiciels permettant le piratage des systèmes de paiement, la fourniture de dispositifs techniques de déchiffrement, la fourniture de logiciel pour « aspirer » sur internet les adresses électroniques de personnes physiques en vue de constituer un fichier de prospects (Cass crim. 14 mars 2006).

CONCLUSION ***(0,5 point)***

Existence d'une conclusion qui réponde à la problématique

La généralisation d'internet et de l'informatique en réseau, donne une nouvelle dimension à la fraude informatique ce qui justifie les lois Godfrain de 1988 et LCEN de 2004. Les entreprises, responsables en matière de traitement des données, ont su mettre en place des dispositifs techniques de sécurisation et se sont adaptées aux dispositifs légaux.
Mais la particularité de la fraude informatique est que le développement des réseaux facilitera toujours sa propagation.

Barème

Il n'est pas question d'exiger que le candidat fournisse toutes les idées mentionnées dans le corrigé.

À titre indicatif, on peut attribuer :
- deux points et demi si le candidat montre que la loi Godfrain est une réponse à la fraude informatique ;
- deux points si le candidat met en évidence les évolutions juridiques nécessaires pour faire face à la fraude ;
- un point si le candidat présente dans sa copie une opposition et/ou une complémentarité d'idées sous forme de deux ou trois parties : les arguments développés doivent véritablement traduire cette opposition ou cette complémentarité (l'annonce d'un plan ne suffit pas pour l'attribution de ce point).

L'examinateur prend aussi en compte la qualité de la rédaction.