

Corrigé et barème – La cybercriminalité et les droits numériques

Connaître les risques en ligne et les droits dans l'espace numérique

Durée : 55 min – Sans document – Sur 20 points · EMC 4^e

Exercice 1 – Notions et repères

(4 pts)

- a) Ensemble des infractions commises au moyen des outils numériques ou contre eux ; exemple contre : piratage d'un serveur, rançongiciel. (1)
- b) Injure = insulte sans fait précis ; diffamation = imputation d'un fait précis portant atteinte à l'honneur. Loi du 29 juillet 1881 sur la liberté de la presse. (1)
- c) Loi pour la confiance dans l'économie numérique, 21 juin 2004 : retirer promptement tout contenu manifestement illicite signalé (et conserver les données de connexion). (1)
- d) Des propos ou comportements répétés, et une dégradation des conditions de vie (santé physique ou mentale). (1)

Repère — 1881, 1978, 2004, 2018, 2022, 2024 : chaque date correspond à un texte et à un problème (presse, fichiers, hébergeurs, données, école, plateformes).

Exercice 2 – Analyse de document : l'article 222-33-2-2 du Code pénal

(4 pts)

- a) Conditions : des propos ou comportements « répétés », ayant « pour objet ou pour effet une dégradation des conditions de vie ». Conséquence : « une altération de sa santé physique ou mentale ». (1)
- b) a) : les auteurs agissent de manière concertée ou sous l'impulsion d'un meneur ; b) : ils agissent successivement sans s'être concertés, mais en sachant que leurs messages s'ajoutent à d'autres. Le raid spontané correspond au cas b). (1)
- c) 3 ans et 45 000 € : deux circonstances aggravantes réunies, le 2° (victime mineure de 15 ans) et le 4° (service de communication en ligne). (1)
- d) Le texte prévoit que l'infraction est constituée « alors même que chacune de ces personnes n'a pas agi de façon répétée » : la répétition est collective ; il suffit qu'il ait su que d'autres écrivaient (cas b). (1)

Méthode — un article de loi se lit en trois temps : la définition (conditions), les cas assimilés, puis l'échelle des peines avec ses circonstances aggravantes numérotées.

Exercice 3 – Lecture d'un tableau : l'échelle des peines

(4 pts)

- a) $12\,000 \div 38 \approx 316$: multipliée par plus de 300. Un groupe de 30 personnes n'est pas un cercle intime lié par une communauté d'intérêts ; les messages peuvent être capturés et diffusés ; la justice y voit une publication. (1)
- b) Harcèlement moral et apologie du terrorisme (l'injure change de régime quand elle devient publique). Raison : en ligne, la diffusion est massive, permanente, atteint la victime partout et ses traces durent. (1)
- c) Apologie du terrorisme (7 ans) > escroquerie (5 ans) > harcèlement moral (2 ans) > usurpation d'identité (1 an) > injure publique (amende seule). (1)
- d) L'escroquerie est bien plus punie (5 ans et 375 000 € contre 1 an et 15 000 €). Le Code pénal punit selon le dommage social et le préjudice financier ; mais l'usurpation sert souvent à commettre une escroquerie : les deux peuvent alors se cumuler. (1)

Attention — les peines indiquées sont des maximums : le juge tient compte de l'âge, du casier et de la gravité, et un mineur voit ces peines divisées par deux.

Exercice 4 – Étude de cas : le compte piraté*(4 pts)*

- a) Le SMS est un hameçonnage : tentative d'escroquerie (art. 313-1, 5 ans et 375 000 €). La connexion est un accès frauduleux à un système de traitement automatisé de données (art. 323-1, 3 ans et 100 000 €), même sans modification. (1)
- b) Oui : Malik fait usage de données permettant d'identifier Inès (son nom, son compte) « en vue de troubler sa tranquillité » et « de porter atteinte à son honneur » (art. 226-4-1, 1 an et 15 000 €) ; les mêmes peines s'appliquent en ligne. (1)
- c) Partager, c'est diffuser à nouveau : ils deviennent auteurs d'une publication injurieuse (« complètement folle ») et, par la répétition à six sur trois semaines, participent à un harcèlement en ligne (art. 222-33-2-2, cas b : chacun sait que d'autres partagent). Leurs parents sont civilement responsables (art. 1242). (1)
- d) Signaler au 3018, qui peut obtenir un retrait rapide ; signaler sur PHAROS ; déposer plainte au commissariat (ou via THESEE pour l'hameçonnage) ; saisir l'Arcom du manquement de la plateforme à ses obligations de traitement des signalements (DSA, 2024) ; demander l'effacement des données auprès de la CNIL (RGPD). (1)

Le point clé — une seule histoire cumule plusieurs infractions distinctes : on les sépare une par une (auteur, acte, texte) avant de chercher les recours.

Exercice 5 – Développement guidé : faut-il interdire l'anonymat sur internet ? *(4 pts)*

- a) Le pseudonyme cache l'identité aux autres utilisateurs, pas à la plateforme : la LCEN (2004) impose la conservation des données de connexion, remises à la justice sur réquisition. L'anonymat total n'existe donc pas. (1)
- b) Exemple attendu : un raid numérique ou une usurpation d'identité sous pseudonyme ; l'identification obligatoire dissuaderait les auteurs, qui se croient impunis, et accélérerait les enquêtes. (1)
- c) Le pseudonymat protège la liberté d'expression (DDHC, art. 11) de personnes exposées : victimes qui témoignent, lanceurs d'alerte, opposants dans des pays autoritaires, mineurs ; il limite aussi le fichage commercial (RGPD). (1)
- d) Le droit actuel préfère la responsabilité a posteriori : identification par la justice via les hébergeurs (LCEN), retrait rapide et transparence de la modération (DSA), sanctions pénales et bannissement (loi SREN, 2024), plutôt qu'un contrôle d'identité préalable de tous. (1)

À retenir — un bon développement d'EMC expose les deux positions avec des faits précis, puis conclut sur ce que prévoit réellement le droit, sans réduire le débat à une opinion.