

<https://www.observatoire-collectivites.org/spip.php?article5415>

# **Intrusion fortuite dans le système informatique d'une administration : l'exploitation d'une faille technique n'est pas une cause d'exonération**

- Jurisprudence -



Publication date: mercredi 20 mai 2015

---

Copyright © Observatoire Smacl des risques de la vie territoriale - Tous

droits réservés

---

**Grâce à une recherche sur internet, un internaute accède à des données confidentielles fortuitement en libre accès sur le site d'une administration. Est-il pénalement responsable s'il télécharge ces documents sensibles en l'absence de tout acte de piratage informatique ?**

[1]

**Oui dès lors qu'il s'est volontairement maintenu dans un système de traitement automatisé après avoir découvert que celui-ci était protégé et a soustrait des données qu'il a utilisées sans le consentement de leur propriétaire. La circonstance que l'intéressé n'ait pas eu besoin de pirater des codes pour accéder aux documents sensibles ne constitue pas une cause d'exonération. Se rend ainsi coupable de maintien frauduleux dans un système de traitement automatisé de données et de vol au préjudice de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES), un internaute qui télécharge des données confidentielles qui se sont retrouvées fortuitement en libre accès à la suite d'une défaillance technique du site. Attention : si l'internaute qui profite d'une défaillance de sécurité engage sa responsabilité pénale, cela n'exonère pas pour autant le responsable du traitement de données personnelles de ses propres responsabilités, celui-ci étant tenu de prendre toutes précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.**

Grâce une recherche sur Google, un internaute arrive par erreur au cœur de l'extranet de l'ANSES, découvrant de nombreux documents confidentiels en libre accès. Il télécharge l'ensemble de ces données sur son serveur afin de les utiliser pour argumenter son article sur la légionellose et en fixe une partie sur différents supports pour les diffuser à des tiers. L'internaute reconnaît avoir parcouru l'arborescence des répertoires du site et être remonté jusqu'à la

page d'accueil où il s'est aperçu de la présence d'un contrôle d'accès.

Il est poursuivi pénalement pour maintien frauduleux dans un système automatisé de données et pour vol.

Pour sa défense l'internaute objecte que c'est une défaillance du système de protection de l'ANSES qui a rendu l'accès libre à ces données et qu'il s'est contenté d'utiliser un moteur de recherche grand public sans acte de piratage.

Peu importe répond la Cour de cassation qui confirme sa condamnation à 3000 euros d'amende dès lors qu'il s'est maintenu dans un système de traitement automatisé après avoir découvert que celui-ci était protégé et qu'il a soustrait des données qu'il a utilisées sans le consentement de leur propriétaire.

[Cour de cassation, 20 mai 2015, NÂ° 14-81336](#)



PS:

– Le maintien dans un système informatique après avoir découvert que celui-ci est protégé est frauduleux, alors même que l'accès s'est fait via un moteur de recherche, et que la sécurité du site est défaillante.

– Constitue un vol le fait de télécharger des données et des fichiers informatiques sans le consentement de leur propriétaire.

– Cette décision peut tout à fait être transposée à un système automatisé de données géré par une collectivité. Victime directe de l'infraction, la collectivité peut alors porter plainte et se constituer partie civile.

– Attention toutefois s'agissant des traitements automatisés de données à caractère personnel. La loi dite "Informatique et Libertés" impose, en son article 34, une obligation de sécurité à la charge du responsable de traitement : "le responsable de traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès."

Si la responsabilité pénale de l'internaute peut être retenue, des sanctions administratives et pénales peuvent également être encourues par le responsable de traitement.

---

## Références

– [Article 323-1 du code pénal](#)

– [Article 311-1 du code pénal](#)

– [Article 34 de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, dite loi "Informatique et Libertés"](#)

## Etes-vous sûr(e) de votre réponse ?

- [La violation de la charte informatique peut-elle constituer un motif légitime de licenciement ?](#)
- [Un maire peut-il utiliser les données du recensement pour mettre à jour le fichier population ?](#)
- [Un directeur général peut-il verser au dossier d'un fonctionnaire un courriel polémique dont il n'était pas destinataire ?](#)

---

[1] Photo : © Valerie Potapova