Criminalité informatique : les nouvelles dispositions du Code pénal suisse sont en vigueur

Autor(en): **Page, Gérald**

Objekttyp: **Article**

Zeitschrift: **Revue économique franco-suisse**

Band (Jahr): **75 (1995)**

Heft 1

PDF erstellt am: **17.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-886513

Criminalité informatique : les nouvelles dispositions du Code pénal suisse sont en vigueur

Gérald Page, docteur en droit, avocat au Barreau de Genève

Les nouvelles normes du Code pénal suisse visant la criminalité informatique sont entrées en vigueur le 1er janvier 1995. Vu leur complexité et leur technicité pour le juriste, leur application n'ira pas sans soulever de nombreuses questions, mais elles constituent un progrès important, dans la ligne de réflexion des législateurs européens.

Le droit pénal suisse classique permettait mal de saisir le comportement criminel informatique, de l'incriminer. L'interprétation restrictive des normes pénales empêchait d'étendre les délits de droit commun à des actes qui n'étaient plus vraiment commis par des hommes ou à l'encontre de choses. L'application des normes fondées sur des concepts classiques (vol, escroquerie, abus de confiance, faux dans les titres) était difficile ou incertaine car elle se heurtait à la notion pénale de la chose (l'information ou la donnée ne sont donc pas des choses) ou celle de la tromperie astucieuse de la victime (l'ordinateur n'est pas une personne). Les manipulations informatiques ne brisent pas la possession, ne détruisent ou n'endommagent pas forcément une chose.

Les délits dans le domaine électronique ont ceci de particulier qu'ils sont invisibles ou difficilement décelables (1) accomplis avec une rapidité extrême, potentiellement sur une grande échelle du fait des possibilités d'interconnexions, sources de préjudices importants dus à la dépendance croissante des activités économiques des systèmes électroniques de traitement et de transmission d'informations, et, souvent, de dimension internationale.

Les nouvelles normes s'inscrivent dans un remaniement important du titre du Code pénal consacré aux délits contre le patrimoine, dans lequel les délits informatiques brisent les catégories classiques. Par ailleurs, le caractère subsidiaire de certaines normes laisse présager de délicats problèmes de concours entre les diverses infractions. Leur nature ouverte, nécessaire afin de pouvoir suivre l'évolution technologique rapide, leur fait perdre en clarté, notamment dans tous les cas où le législateur n'a eu d'autre alternative que de viser des « procédés analogues, similaires ».

La notion de « donnée » est l'élément central de la révision. Elle n'est pas définie spécifiquement dans le code. L'interprétation des nouvelles normes montre cependant qu'elle se situe à mi-chemin entre une notion matérielle et immatérielle, car, étant une représentation de l'information et non l'information elle-même, elle est quand même susceptible de soustraction ou d'appropriation. Le **logiciel** est considéré pénalement comme un ensemble de données, de sorte qu'il ne fait pas l'objet d'un traitement spécifique (sous réserve des dispositions pénales contenues dans la loi sur le droit d'auteur dans les cas de contrefaçons).

La révision a donc créé quatre types d'infractions nouvelles :

❑ L'escroquerie informatique (« utilisation frauduleuse d'un ordinateur », art. 147 CP)

L'article 147 CP réprime l'escroquerie commise au moyen d'un ordinateur, soit l'acte de celui qui, astucieusement, influe sur un processus électronique de traitement ou de transmission de données, pour en modifier le résultat de manière à provoquer un transfert d'actifs, l'acte étant commis avec le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime. L'acte est commis en utilisant des données de manière incorrecte, incomplète ou indue. Il permet par exemple d'appréhender le comportement de celui qui utilise la carte de crédit ou d'identification falsifiée d'un tiers et introduit ainsi de fausses données dans un système sur la validité de la carte, les limites de crédit, etc. C'est le lieu de rappeler que la révision a

1) Les délits informatiques n'entraînent souvent aucune activité ou interaction physique ou personnelle ; l'ordinateur peut être facilement utilisé non seulement pour commettre l'infraction mais également pour en effacer les traces ou les preuves ; les délits sont le plus souvent perpétrés par des « insiders », précisément par ceux qui seraient le mieux à même de détecter et prévenir l'activité délictuelle ; lorsqu'il est découvert, le délit ne fait souvent pas l'objet d'une dénonciation de par l'effet très négatif sur les exploitants ayant la responsabilité de gestion de patrimoines importants ; lorsqu'il est dénoncé, la poursuite du délit est souvent difficile.

également donné naissance à un nouvel article 148 CP qui réprime l'abus de carte-chèques et de cartes de crédit (par leur titulaire).

❑ L'espionnage informatique (« soustraction de données », art. 143 CP, « accès indu à un système informatique », art. 143bis CP)

La soustraction (« vol ») de données (art. 143 CP)

Est réprimé d'office par cette disposition l'acte de celui qui soustrait des données dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime. Le bien pénalement protégé n'est pas la donnée elle-même, mais le droit de maîtrise de l'exploitant sur ses données, libre d'ingérence de tiers. Celui qui ne le fait que par jeu, donc sans dessein d'enrichissement, n'est poursuivable que du chef d'accès indu à un système informatique (art. 143*bis* CP) ou, s'il a modifié les données, du chef de détérioration de données (art. 144*bis* CP). Il y a soustraction également lorsque les données ne sont que copiées et qu'elles ne subissent aucune modification. L'acte n'est cependant punissable que s'il s'agit de données enregistrées ou transmises électroniquement ou selon un mode similaire, si la soustraction a lieu sans droit, c'est-à-dire que les données ne sont pas destinées à l'auteur, et si celles-ci étaient spécialement protégées contre tout accès indu de l'auteur. Celui qui s'accapare des données sur un réseau ou dans un système qui ne dispose d'aucune protection, et qui n'a donc aucune barrière ou porte à franchir pour le faire, n'est pas punissable. Une transmission de données non cryptées sur un réseau public ne bénéficierait donc pas de cette protection pénale en Suisse (les dispositions sur le secret des communications et les écoutes téléphoniques demeurant réservées).

L'accès indu à un système informatique (art. 143bis CP)

Est punissable au sens de cette disposition l'acte de celui qui s'introduit sans droit dans un système au moyen d'un dispositif de transmission de données, même par jeu, ou sans dessein de nuire ou d'enrichissement ou sans provoquer de dommage. L'auteur n'est cependant punissable que si le système en question était spécialement protégé contre tout accès indu. Il n'est pas punissable s'il prend connaissance sur place de données, par exemple à l'écran ou sur imprimante, sans mettre en œuvre de dispositif de transmission.

❑ Le sabotage informatique (« détérioration de données », art. 144bis CP)

Est réprimé l'acte de celui qui cause une altération des données d'autrui, quelle que soit l'importance de cette altération ou la valeur des données. Le délit pourrait donc être commis également lorsque des données sont ajoutées et non pas seulement lorsqu'elles sont effacées. Si la victime subit un dommage considérable, la sanction est aggravée et la poursuite a lieu d'office. Le nouvel article 172*ter*, allégeant la sanction dans les cas d'infractions d'importances mineures, est applicable. L'on peut songer à celui qui a modifié des données par jeu ou défi, sans causer un quelconque préjudice à l'exploitant et qui est en mesure de rétablir immédiatement l'état antérieur.

La disposition vise manifestement l'introduction d'un virus dans un système. L'art. 144*bis* al. 2 CP réprime en outre spécifiquement la fabrication, l'importation, la mise en circulation, la promotion ou l'offre, la mise à disposition de quelqu'autre manière de logiciels dont l'auteur savait ou devait présumer qu'ils devaient être utilisés dans le but de procéder à une détérioration de données.

❑ Le vol de temps machine (« obtention frauduleuse d'une prestation », art. 150 CP)

La disposition vise l'acte de celui qui utilise un ordinateur ou un appareil automatique, obtenant ainsi sans bourse délier une prestation dont il savait qu'elle n'est fournie que contre paiement.

❑ Le faux dans les titres électroniques (art. 251 et 110 ch.5 al. 1 CP)

La révision met fin à une longue controverse quant à la qualité de titre des documents électroniques. L'article 110 ch. 5 al. 1 CP précise aujourd'hui que **sont réputés titres tous écrits destinés et propres à prouver un fait ayant une portée juridique et tous signes destinés à prouver un tel fait, l'enregistrement sur des supports de données et sur des supports images étant assimilé à un écrit,** s'il a la même destination. La loi ne fait donc plus dépendre la qualité de titre de l'aspect extérieur visible. Il faut cependant que le titre électronique possède les fonctions inhérentes et nécessaires à la notion classique de titre, comme par exemple la fixation de l'expression de la pensée humaine, la reconnaissabilité du créateur du titre (fonction de garantie), perpétuité, adéquation et fonction de preuve. La falsification d'un titre électronique peut donc faire l'objet d'une poursuite pénale pour faux (art. 251 CP).

*
* *

Il reste à observer l'évolution des nouvelles normes dans la révolution télématique actuelle, le multimédia, les autoroutes de l'information, etc. Les premiers projets de révision étaient fondés sur une notion plus structurelle et statique de l'informatique. Les experts ont cependant très vite constaté que l'informatique moderne est autant le traitement que la transmission de l'information, en particulier si l'on se souvient que des traitements toujours plus nombreux ont lieu à distance. C'est donc à juste titre que les nouvelles dispositions pénales étendent leur protection également à la phase de la transmission des données, celle qui, au demeurant, est la plus sensible et la plus vulnérable. ■