TF, 24.06.2026, 6B_120/2026*

Un employé qui exploite une faille de sécurité sur son espace de travail pour accéder sans droit à un espace informatique de son employeur réservé à un groupe de collaborateurs se rend coupable d'accès indu à un système informatique au sens de l'art. 143bis CP.

Faits

Au moyen d'un script, un employé exploite une faille informatique « Oracle » afin d'élever ses privilèges au rang d'administrateur (*privilege escalation*) et installe un logiciel non autorisé sur son poste de travail au lieu de déposer une demande d'accès selon les procédures de l'entreprise. L'employeur dépose plainte.

Le Tribunal correctionnel de l'arrondissement de la Broye et du Nord vaudois libère l'employé du chef de prévention d'accès indu à un système informatique (art. 143bis CP). Sur appel du Ministère public, la Cour d'appel pénale du Tribunal cantonal vaudois réforme le jugement et condamne l'employé pour cette infraction.

L'employé forme recours en matière pénale auprès du Tribunal fédéral. Celui-ci doit examiner si l'exploitation d'une faille de sécurité permettant une élévation de privilèges constitue un accès indu à un sous-système informatique réservé à certains ayants droit au sens de l'art. 143bis CP.

Droit

Se rend coupable d'accès indu à un système informatique (art. 143bis CP) quiconque s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part. Cette infraction constitue un acte préparatoire à la soustraction de données (art. 143 CP), mais vise les systèmes ou installations de traitements et non les données stockées.

La notion de « système informatique » comprend non seulement l'ordinateur, mais également les installations et espaces virtuels de traitement de données, ainsi que les sous-

systèmes au sein d'un système informatique auxquels l'auteur n'a pas accès.

Cette conception large s'impose pour plusieurs motifs, notamment le fait que le législateur a délibérément remplacé le terme « ordinateur » par celui de « système informatique » par rapport au projet initial du Conseil fédéral afin de faire bénéficier les données d'une protection pénale au travers de la protection des systèmes de traitement et d'anticiper l'évolution technologique. En outre, une interprétation de l'art. 143bis CP conforme à l'art. 2 de la Convention sur la cybercriminalité (CCC), qui punit l'accès « à tout ou partie » d'un système informatique, plaide pour la protection pénale des sous-systèmes. Finalement, par analogie avec l'infraction de violation du domicile (art. 186 CP) qui protège la paix du domicile, la paix informatique couvre chaque espace virtuel fractionné du système informatique. Dans le même sens, le Tribunal fédéral a déjà considéré que le compte de messagerie électronique d'un tiers constitue une partie de système informatique appartenant à autrui (ATF 145 IV 185 c. 2.3 résumé *in* LawInside.ch/774/).

La condition de la protection spéciale du système informatique découle de la réserve de la Suisse à l'art. 2 CCC, laquelle exige le contournement d'un système de protection de l'accès. L'ayant droit doit manifester sa volonté d'empêcher les tiers d'accéder au système informatique, notamment par des codes d'accès, un chiffrement ou un mot de passe. Les mesures de protection doivent correspondre aux normes de sécurité habituelles et être raisonnablement exigibles de l'exploitant du système au regard des circonstances concrètes. Ces mesures n'ont pas à atteindre l'optimum de la technique, au vu des avancées des pirates informatiques. La présence d'une faille de sécurité n'exclut pas l'existence d'une protection spéciale, car de telles vulnérabilités sont fréquentes.

Le comportement d'intrusion consiste à contourner les barrières d'accès qui visent à empêcher l'auteur d'accéder au système. En principe, la manière dont l'auteur désactive la sécurité importe peu, pour autant que son acte soit propre à la désactiver et sans qu'un investissement particulier en temps ou en moyens techniques ne soit nécessaire. La notion d'accès sans droit se recoupe avec celles de système appartenant à autrui et de protection spéciale, et permet en outre d'exclure du champ d'application de l'art. 143bis CP le piratage

éthique (*ethical hacking*) ou les services de sécurité informatique.

Du point de vue subjectif, l'infraction est intentionnelle, le dol éventuel étant suffisant. L'auteur doit avoir conscience d'accéder à un système informatique protégé auquel il n'a pas droit et de contourner une barrière d'accès.

En l'espèce, l'espace informatique auquel l'employé a accédé, dont l'accès est restreint aux détenteurs des droits d'administrateur, permet l'installation de *drivers*. Puisque le système informatique de l'employeur est fractionné en différents espaces avec un accès délimité selon le statut des personnes, ce sous-système constitue un système informatique au sens de l'art. 143bis CP. L'employé n'appartient pas au groupe de collaborateurs disposant des droits d'accès correspondants. Dès lors, le sous-système appartient à autrui, peu importe que l'employé se soit connecté à sa propre session au moyen de ses propres identifiants, dès lors que le sous-système auquel il a accédé doit être distingué de sa propre session.

Par ailleurs, le sous-système est spécialement protégé. La faille exploitée suppose précisément l'existence d'une protection destinée à en limiter l'accès. La réalisation d'un audit interne concernant la faille « Oracle » et sa correction par le service informatique permettent de retenir que les mesures de protection en place correspondent aux normes techniques de sécurité habituelles, ce que confirme l'existence d'une procédure interne de demande d'augmentation des droits.

De plus, l'utilisation d'un script par l'employé pour exploiter la faille de sécurité vaut usage d'un dispositif de transmission de données au sens de l'art. 143bis CP et constitue un acte d'intrusion. Quant au caractère sans droit de l'accès, l'employé ne conteste pas l'existence d'un mécanisme de gestion des demandes d'accès qu'il n'a pas respecté et admet que son comportement est contraire à la procédure habituelle d'élévation des privilèges informatiques.

Sur le plan subjectif, la volonté de l'employé de « gagner du temps » et l'absence d'intention de perturber le système ou de soustraire des données importent peu, car les desseins et motivations de l'auteur ne sont pas pertinents. Ainsi, l'employé réalise les éléments

constitutifs de l’infraction d’accès indu à un système informatique au sens de l’art. 143bis CP.

Le Tribunal fédéral rejette tous les griefs de fond, mais admet très partiellement le recours concernant la mise à charge des frais et le refus d’allouer des indemnités à l’employé.

Proposition de citation : Nadia Masson, L’accès indu à un système informatique par « privilege escalation » (art. 143bis CP), in: https://lawinside.ch/1768/