Le scan de ports : une intrusion dans un STAD ?

Par Xavier LEMARTELEUR
Juriste spécialisé en droit des technologies de l'information
Email : xlemarteleur@vaevictis.org

Les actes d'intrusion informatique sont sanctionnés pénalement depuis la loi Godfrain de 1988 au travers de l'article 323-1 du Code pénal qui incrimine le fait « *d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* »(STAD). Récemment, les sanctions associées à ce délit ont été largement relevées par la loi pour la Confiance dans l'Economie Numérique. La peine associée à une intrusion informatique est désormais de deux ans de prison et 30 000 euros d'amende. Cette sanction est d'ailleurs renforcée s'il a résulté de cette intrusion la suppression ou la modification[1] de données contenues dans le système : dans ce cas, la sanction est portée à trois ans d'emprisonnement et 45 000 euros d'amende.

Si les contours de la notion d'intrusion informatique semblent aisément traçables, en pratique la qualification pénale d'accès frauduleux dans un STAD peut poser certaines difficultés. En effet, en informatique comme dans la vie réelle, il existe tout un panel de comportements qui se trouvent à la frontière de l'incrimination pénale. Tel est notamment le cas du scan de ports d'une machine distante.

D'abord faut-il sans doute préciser, pour le juriste qui ne serait pas à l'aise avec les considérations techniques, ce qu'est un « scan de port ».

Le scan de port est une « *technique consistant à balayer automatiquement, à l'aide d'un programme approprié, une série d'adresses IP spécifiques afin de trouver et d'examiner les ports ouverts sur chaque ordinateur, puis d'exploiter ces failles de sécurité en vue d'une intrusion. (…) Le scannage de ports est également utilisé par les administrateurs de système pour vérifier les failles de sécurité* »[2].

Les « ports » sont des points d'entrées par lesquels une machine va pouvoir communiquer et échanger des informations avec d'autres ordinateurs. De manière générale à chaque service en fonction sur la machine correspondra un port différent[3]. Ce port sera ouvert si le service est utilisé et chaque port ouvert constitue un point d'accès possible vers la machine (comme une porte restée ouverte).

Identifier les ports ouverts est un moyen de connaître les services existants sur une machine distante. Mais pour le pirate, chaque port ouvert offre également une opportunité supplémentaire de pénétrer frauduleusement dans un système. Il constitue souvent un préalable à un acte d'intrusion. Toutefois, le scan de port doit-il être considéré comme une tentative d'intrusion sanctionnée au titre de l'article 323-1 du Code pénal ?

Considérations pratiques

S'il est certain que la technique du scan de port peut être le préalable à une attaque, tel n'est pas toujours le cas. Certaines actions peuvent ainsi être effectuées de manière parfaitement légitime (un administrateur scanne ses machines pour identifier les logiciels utilisés dans son entreprise, dans le cadre de la réalisation de tests d'intrusion – pentest - ou par de simples curieux notamment des personnes soucieuses de la sécurité qui souhaitent vérifier qu'une machine hébergeant des données est bien sécurisée).

[1] Ce qui normalement, si l'on prend la chose dans son sens strict, sera toujours le cas, la machine enregistrant dans ses logs les actions réalisées, ou le pirate effaçant ces logs dans un objectif « *anti-forensics* » (c'est à dire de techniques permettant de maquiller les traces du passage du pirate).
[2] http://www.olf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/Internet/fiches/8363610.html
[3] A ce port est associé un numéro permettant de l'identifier. Les ports les plus usités sont le port 80 pour le protocole HTTP servant au Web, 21 pour le protocole FTP utilisé pour le transfert de fichiers, 110 pour le protocole POP utilisé pour consulter les courriers électroniques…

Peut être est-il plus facile de comprendre la problématique liée à la question de la légalité des scans de ports en raisonnant par analogie, en comparant le système informatique à un domicile[4].

Un individu qui s'avère, par ailleurs, être expert en assurance et connaît bien les systèmes de sécurité mis en place pour sécuriser les logements (serrures, système d'alarme,…), se promenant dans la rue (sans avoir l'intention de commettre une effraction), peut être amené à exercer sa curiosité sur la sécurité des habitations qu'il croise. Il pourra, par exemple, noter qu'une porte ne semble pas très solide ou encore aller voir le barillet de la serrure pour relever sa marque et constater, au vu de ses connaissances, que cette serrure comporte un défaut qui permettrait à un cambrioleur de pénétrer dans la demeure.

Ce type de comportement pourrait être largement assimilé à un simple scan de port d'une machine distante. La personne curieuse va interroger une machine pour connaître certaines informations sur son état. Les éléments ainsi révélés ne devraient pas caractériser une intrusion dès lors que les informations collectées sont de caractère « public ».

Il semble opportun d'effectuer une distinction entre ce qui devrait être considéré comme donnée « publique » et ce qui relève de l'ordre « privé » de la machine.
La donnée publique serait celle qui peut être connue par une interaction normale avec le système d'information et dont la connaissance peut être nécessaire notamment à des fins d'interopérabilité, par opposition aux informations « privées » de la machine qui seraient constituées notamment des données qu'elle est amenée à traiter (par exemple les données qu'elle stocke ou les logiciels qu'elle comporte).
Concrètement lors d'un échange entre deux machines, la structure des réponses formulées par la machine interrogée ou encore, plus prosaïquement, le contenu direct de ses réponses peuvent permettre de connaître certaines informations révélant son « identité ». Ces informations techniques sont nécessaires aux ordinateurs afin de pouvoir établir entre eux une connexion et échanger des informations.

Une autre analogie permet de mieux illustrer ce point : si un individu appelle une personne qu'elle ne connaît pas au téléphone, elle peut en tout état de cause disposer d'informations relatives à cette personne permettant non pas de l'identifier directement mais de connaître ou de déduire quelques-unes de ses caractéristiques telles que : sa localisation géographique (déduite du numéro de téléphone appelé), son sexe (voix), son origine géographique (accent). Il ne s'agit pas ici d'une véritable intrusion dans la vie privée mais de données qui transparaissent naturellement de l'échange.

Dans le cas de l'interaction entre deux systèmes, le même type de déduction peut être réalisé, ce qui permet de connaître certaines informations relatives à la machine (système d'exploitation[5], ports ouverts et services associés, etc.). Le fait de recueillir ce type d'information ne devrait pas être sanctionnable étant donné que ces informations ne relèvent pas de l'« intimité » de la machine mais sont, et doivent être, publiquement accessibles afin de permettre la communication entre les machines distantes (notamment afin de reconnaître le protocole informatique utilisé…).

Le fait que l'utilisateur n'ait pas généralement à connaître ces informations, ne doit pas être un élément à considérer. Il est cependant certain que ce type de démarche peut s'inscrire dans le contexte de la préparation d'une attaque contre un système d'information. A ce titre, quel est le risque auquel s'expose le « scanneur » ? Sa « curiosité » pourrait-elle lui valoir des poursuites pénales pour accès ou tentative d'accès frauduleux à un STAD ?

Le scan de port : un accès à un STAD ?

La question paraît devoir recevoir une réponse clairement négative. En effet, de part son fonctionnement, le scan de port ne saurait être considéré comme un « accès » à un système

[4] Sans vouloir plus particulièrement rentrer dans le débat de l'assimilation du système d'information à un « domicile virtuel ».
[5] On parle généralement en langage technique d' « *OS fingerprinting* ».

d'information : les opérations réalisées lors du scan se cantonnant à une interaction [6]avec la machine ciblée, l'incrimination prévue par l'article 323-1 du Code pénal ne saurait être retenue. Les données recueillies étant « publiques », c'est-à-dire librement accessibles comme nous avons pu le voir *supra*, elles ne sauraient être qualifiées de confidentielles et leur collecte ne nécessite normalement pas que soit contourné un système de protection. Or, selon la jurisprudence, ces deux éléments semblent conditionner la poursuite pénale de l'intrusion[7].

Ce qui fait ici défaut, c'est l'élément intentionnel de l'infraction. Rappelons qu'en droit pénal il est nécessaire, pour que le comportement puisse être sanctionné, que trois éléments soient réunis : un élément légal (le fait que l'acte soit réprimé pénalement[8]), un élément matériel (c'est à dire une exécution ou un début d'exécution[9]) et enfin un élément intentionnel (le fait de commettre l'acte répréhensible sciemment[10]). Or, en l'absence de contournement d'un dispositif de sécurité ou de la connaissance du caractère confidentiel des informations accédées, il ne semble pas que l'on puisse caractériser l'intention de l'auteur de commettre une infraction.

On notera que si, en France, cette question n'a pas encore été tranchée par la jurisprudence, dans d'autres ordres juridiques, celle-ci a depuis plusieurs années été abordée. Ainsi un tribunal américain avait été saisi d'une affaire mettant en cause une personne ayant scanné des machines. La juridiction a considéré que ce scan n'était pas sanctionnable. Le juge relève ainsi : « [T]*he tests run by Plaintiff Moulton did not grant him access to Defendant's network*. (…) *The public data stored on Defendant's network was never in jeopardy*»[11].

Accessoirement, au regard du droit français, le risque pénal que pourrait encourir le « scanneur » serait que le scan soit considéré comme une action entravant le fonctionnement du système d'information (sanctionné par l'article 323-2 du Code pénal). Cependant une telle qualification semble assez improbable étant donné que le scan de ports, s'il demeure isolé, ne mobilise pas de ressources importantes pour la machine ciblée tant au niveau du trafic réseau généré que de l'utilisation de puissance de calcul de la machine cible.

Cette question tranchée, on peut se demander si le simple scan de port pourrait être un élément suffisant pour constituer un début de réalisation matérielle de l'infraction d'accès à un STAD ?
Le scan en lui-même ne pourrait être considéré comme la réalisation matérielle de l'infraction (dans le sens où il ne constitue pas en tant que tel une intrusion comme cela a été exposé préalablement). Par contre, il sera souvent, comme nous avons pu le souligner, un des prémices à l'infraction[12]. Reste à déterminer si celui-ci peut être suffisant pour constituer une tentative d'intrusion.

Le scan de ports: une tentative d'intrusion ?

Rappelons que l'article 323-7 du Code pénal prévoit que « *la tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines* ». Cet article doit être mis en relation avec l'article 121-5 du même code qui dispose que « *la tentative est constituée dès lors que, manifestée par un commencement d'exécution, elle n'a été suspendue ou n'a manqué son effet qu'en raison de circonstances indépendantes de la volonté de son auteur* ».

---

[6] Dans ce sens, le scan est comparable au « Ping » qui permet en envoyant une requête à une machine distante et en mesurant son temps de réponse de connaître l'état du réseau ou la charge de la machine hôte.
[7] Dans ce sens : voir la décision CA Paris, 11ème Chambre, 8 décembre 1997 et la décision émanant de la même cour du 30 octobre 2002 « Kitetoa ». Dans la dernière espèce la cour a décidé qu' « *il ne peut être reproché à un internaute d'accéder aux, ou de se maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès* ».
[8] Article 111-3 du Code pénal.
[9] Article 121-1 Code pénal : « Nul n'est responsable pénalement que de son propre **fait** ».
[10] Article 121-3 du Code pénal.
[11] US district court of Georgia, Moulton v. VC3, 2000 WL 3331091 (N.D. Ga., Nov. 7, 2000). Voir notamment l'article de K. Poulsen, « *Port scan legal, judge says* », disponible à l'adresse suivante : http://www.securityfocus.com/news/126
[12] Dans le cas uniquement où le scan est réalisé dans une intention malicieuse, ce qui rappelons le ne correspond pas à l'ensemble des situations.

Le scan de port constitue-il déjà un « *commencement d'exécution* » au sens de la loi et est-il donc punissable au titre de la tentative ou n'est-il qu'un un simple « acte préparatoire » qui, selon la jurisprudence, ne saurait être sanctionné ?

La distinction entre ces deux phases du délit est assez ténue[13], la frontière entre l'acte préparatoire (non punissable) et le commencement d'exécution (réprimé sous l'angle de la tentative) semble difficile à déterminer.

Selon la Cour de cassation, la qualification de tentative est une question de droit qui relève de son contrôle. Celle-ci a ainsi estimé que le commencement d'exécution devait être défini comme « *l'acte qui tend directement au délit lorsqu'il a été accompli avec l'intention de le commettre* »[14]. Cette définition renvoie donc directement à l'élément moral de l'infraction : est une tentative un acte qui a été accompli sciemment... L'élément matériel de la tentative est caractérisé par l'élément moral du délit et la boucle est bouclée…. On relèvera que l'existence d'un commencement d'exécution dépend largement des faits de chaque espèce[15]. En l'absence de jurisprudence dans le domaine des scans de ports, la question reste ouverte. Il ne semble pas que le scan puisse constituer un acte permettant de prouver un commencement d'exécution et quant à l'élément moral de la tentative, sa preuve sera souvent difficile à apporter[16]. A contrario, il y aura bien tentative d'intrusion dès lors qu'il est prouvé que le « pirate » agissait dans le but de pénétrer dans le système.

Il convient, en dernier lieu, de s'interroger dans cette étude sur le fait de savoir si la détention d'un outil permettant d'effectuer des scan de port est en elle-même constitutive d'une infraction pénale.

La détention d'un logiciel de scan de ports : un délit en tant que tel ?

Introduit par la loi pour la Confiance dans l'Economie Numérique[17] l'article 323-3-1 du Code pénal prévoit que « *le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* ».

A la lecture de cet article, on notera que le champ d'application de l'incrimination est doublement limité : les actes sanctionnés concernent la détention ou la diffusion d'outils de piratage ; mais à la condition que ces outils aient été créés ou modifiés afin de commettre une infraction.

Les logiciels permettant le scan de port doivent-ils ainsi être considérés en tant que logiciels « *conçus ou spécialement adaptés* » pour commettre une infraction ? Répondre par l'affirmative semble assez réducteur et reviendrait à supposer que tous les logiciels développés afin de scanner les ports ont été conçus dans le seul objectif de commettre des actes d'intrusion. En pratique, tel n'est évidemment pas

[13] Sur ce point voir « Droit pénal général », F. Desportes et F. Le Gunehec, corpus de droit privé, Ed. Economica, douzième édition, N° 449 et s.
[14] Cass. Crim. 5 juillet 1951.
[15] Le commencement d'exécution a ainsi été retenu concernant une fausse déclaration s'agissant d'un délit d'escroquerie à l'assurance (Cass. Crim, 1er juin 1994).
[16] L'auteur du scan pourrait ainsi aisément invoquer un moyen de défense appelé « *trojan defense* » en prétextant une infection de son ordinateur par un virus (certains virus comme Nimda effectuant automatiquement des scans des machines sur le réseau) ou encore une prise de contrôle par un tiers. Ce type de moyen de défense a été utilisé avec succès dans plusieurs affaires outre-Manche et notamment en 2003 dans l'affaire Regina v. Caffrey (Regina v Aaron Caffrey, Southwark, Crown Court, 17 October 2003).
[17] Si la LCEN introduit bien cet article dans notre droit, il n'en demeure pas moins que l'origine de l'insertion de cet article trouve une double explication. D'une part, il est inspiré des dispositions de la Loi sur la Sécurité Quotidienne introduisant un article 163-4-1 dans le Code monétaire et financier, sanctionnant le détention et la fourniture de tout élément pouvant servir à falsifier des cartes bancaires. D'autre part, cette disposition avait été incluse dans l'article 6 de la convention cybercriminalité du Conseil de l'Europe (cette dernière disposition étant elle-même inspirée des provisions instaurées par la Convention européenne sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel et par la directive 98/84/EC du Parlement européen et du Conseil en date du 20 novembre 1998 concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel).

le cas et certains de ces outils ont été réalisés non pas à des fins délictueuses mais dans un objectif inverse de sécurisation des réseaux.

On peut donc s'interroger sur la volonté réelle du législateur lors de l'adoption de cette nouvelle incrimination. En l'occurrence, le législateur entendait-il interdire la détention sans motifs légitimes de tout outil pouvant servir à commettre les infractions prévues par les articles du Code pénal en matière d'atteinte aux STAD ou cette incrimination ne concerne-t-elle que les outils véritablement et exclusivement conçus ou modifiés pour commettre ces infractions ?

Il convient ici de procéder à une interprétation de la loi pénale sous deux angles différents : une interprétation téléologique, prenant en considération les vœux du législateur tels qu'ils ressortent des travaux parlementaires, et une interprétation littérale, d'autre part, se limitant au strict contenu de la loi pénale.

Interprétation téléologique de l'article 323-3-1

Il ressort de l'analyse des débats parlementaires ainsi que des différents travaux et rapports produits dans le cadre du processus législatif que la volonté première du législateur était de permettre de lutter contre un phénomène bien connu qu'est la transmission de virus au travers des réseaux ouverts et plus spécifiquement de sanctionner les personnes créant et distribuant des virus informatiques. Si le législateur semble reconnaître qu'il peut exister d'autres programmes informatiques susceptibles d'entrer dans le champ de cette nouvelle incrimination pénale, il ne prend pourtant pas en considération les pratiques pourtant courantes dans le domaine de la sécurité informatique.

Certes, le choix de retenir une dénomination générale, plutôt que de viser explicitement les virus informatiques peut trouver une justification dans un souci de neutralité technologique[18]. Reste que les parlementaires ne semblent pas avoir clairement envisagé, en centrant le débat sur le cas le plus caricatural que sont les virus, le risque que pouvait comporter l'utilisation d'une notion aussi large que celle d' « *équipement, instrument, programme informatique ou toute donnée conçus ou spécialement adaptés* » pour commettre une infraction, et ce même si certains parlementaires ont mis en avant cette difficulté.

Face aux arguments exposant les difficultés pouvant être rencontrées par les professionnels de la sécurité notamment, les défenseurs du texte ont mis en avant l'exception censée les exclure du champ d'application de la disposition tout en reconnaissant qu'il appartiendra en réalité au juge de dresser les contours des « motifs légitimes » pouvant justifier de la détention de tels outils[19].

Interprétation littérale de l'article 323-3-1

A s'en tenir à une lecture stricte du texte de l'article 323-3-1 du Code pénal, on ne peut que constater ses vastes perspectives d'application. En effet, sont sanctionnées la détention ou la cession d'outils de piratage dès lors qu'elles ne sont pas justifiées par des motifs légitimes. L'exception de « motifs légitimes » prévue par le législateur est particulièrement difficile à cerner et devrait être déterminée au cas par cas par le juge. Si, dans certains cas, l'existence de motifs légitimes devrait être aisément acceptée, comme par exemple dans le cas de la détention par un expert de la sécurité informatique dans le cadre de l'exécution de sa mission, il est toutefois des situations dans lesquelles cette exception sera sans doute plus difficilement accueillie (s'agissant cette fois non pas d'un expert reconnu mais d'un simple amateur des questions de sécurité).

---

[18] On notera tout de même sur ce point que les dispositions pénales relatives à la répression de la cybercriminalité en vigueur en Russie, comprennent une disposition claire et explicite qui ne vise que les virus informatiques. Voir le chapitre 28, art. 273 du Code pénal de la Fédération de Russie dont une traduction non officielle est disponible à l'adresse suivante :
http://www.russian-criminal-code.com/PartII/SectionIX/Chapter28.html

[19] L'avis rendu par la commission des lois pour le Sénat précise ainsi : « *Naturellement, la recherche scientifique et la sécurisation des réseaux pourraient entrer dans le champ des motifs légitimes. Il reviendrait au juge d'apprécier la légitimité des motifs, dès lors qu'il est impossible dans la loi d'envisager toutes les hypothèses dans une telle matière* ». Avis n° 351 (2002-2003) de M. Alex TÜRK, fait au nom de la commission des lois, déposé le 11 juin 2003.

Quant aux outils visés par l'incrimination, la notion de « donnée conçue ou modifiée » pour commettre des infractions renvoie par contre à un élément intentionnel à savoir l'objectif recherché par le développeur du programme[20]. Afin d'apprécier si un logiciel répond à la « définition » légale fixée dans l'article 323-3-1 du Code pénal, il conviendrait de rechercher les applications pratiques qui peuvent en être faites (utilisation à des fins de sécurité ou utilisation à des fins de piratage informatique). Ce n'est que dans le cas où l'outil logiciel permet à la fois d'accomplir des actes malveillants et des actes légitimes[21] que l'on pourrait rechercher dans l'intention de l'auteur un élément permettant de déterminer si le logiciel a été spécialement conçu pour commettre des infractions. Dans ce contexte, les outils créés par les entreprises agissant dans le secteur de la sécurité pourraient facilement être exclus du champ d'application de l'article 323-3-1, par contre, les outils issus de développeurs indépendants[22] pourront sans doute plus aisément être considérés comme entrant dans le cadre de l'incrimination.

S'il est vrai que de nombreux outils logiciels conçus et développés par la communauté des experts en matière de sécurité des systèmes d'information peuvent être utilisés à des fins malveillantes par des personnes mal intentionnées, il n'en demeure pas moins que ces outils ont été conçus dans l'objectif de garantir la sécurité des architectures informatiques. Dans ce contexte leur détention ne saurait entrer dans le champ d'application de l'article 323-3-1[23]. Selon nous la rédaction adoptée par cet article du Code pénal ne permettrait d'inclure dans le champ de l'interdiction de détention que certains outils spécifiques dont le seul objectif serait de commettre des actes malveillants. Il en va ainsi des programmes tels que les virus, les troyens, ou les scripts s'appuyant sur des exploits connus.

Ce n'est que pour ces cas particuliers que la détention serait conditionnée à l'existence d'un « motif légitime ».

Conclusion

Le scan de ports doit-il être considéré comme une intrusion dans un STAD ? La réponse à cette question devrait être clairement négative. Toutefois la situation est plus confuse lorsque l'on s'interroge sur la qualification du scan de ports en tant que tentative d'intrusion. Si l'on peut être amené à penser qu'un tel comportement ne devrait pouvoir être qualifié pénalement, il n'existe toutefois pas de décision de jurisprudence dans ce domaine particulier. La personne effectuant un scan d'une machine distante sans autorisation s'expose donc à risque pénal, même si celui-ci demeure assez limité.

Le risque pénal lié à la détention d'outils pouvant servir à commettre des infractions semble par contre plus réel. Toutefois, comme nous avons pu le voir, cette qualification sera dépendante de l'interprétation des tribunaux. Or, à l'heure actuelle la jurisprudence reste encore inexistante sur cette question...

X.L.

---

[20] On rattacherait, de manière assez paradoxale, l'intention l'auteur du logiciel à l'élément intentionnel de l'infraction de détention d'outils informatiques prohibés. Le délit de détention étant a priori un délit objectif (la simple détention sans motif légitime est condamnable même s'il n'existe pas d'intention de commettre une intrusion), c'est l'intention de l'auteur du logiciel qui permettrait de déterminer l'existence de l'élément intention de l'infraction.

[21] Le logiciel pourrait être ainsi comparé aux biens à « double usage » (qui ont une finalité tant civile que militaire) comme par exemple la cryptographie.

[22] Un des logiciels les plus réputé, dénommé NMAP, est ainsi décrit par son auteur (qui s'avère être par ailleurs un expert en matière de sécurité des systèmes d'information) : « *Nmap ("Network Mapper") is an open source tool for network exploration and security auditing (…). While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime* ». L'objectif du développement de NMAP était donc la sécurité et l'audit des réseaux et non le piratage informatique ce qui ne saurait faire de ce logiciel un « *programme informatique (…) conçu ou spécialement adapté pour commettre une ou plusieurs des infractions* [prévues par le Code pénal] » entrant dans le champ de l'article 323-3-1.

[23] La formulation adoptée par l'article 323-3-1 démontre bien à quel point le législateur semble peu familier des pratiques et des mœurs existants dans le secteur de l'informatique.