CAS CONCRET : UNE AFFAIRE JUDICIAIRE MAIS AUSSI ÉCONOMIQUE

PHILIPPE LAURIER
responsable de séminaire à l'École polytechnique, chercheur à l'IRT SystemX

Mafias des pays de l'Est, petits génies du clavier, djihadistes… notre représentation imagée du pirate informatique tient à la fois de la criminologie et de la mythologie. Loin du romanesque de cette représentation, la présentation d'un cas concret de piratage informatique permet de replacer les choses à leur juste proportion.

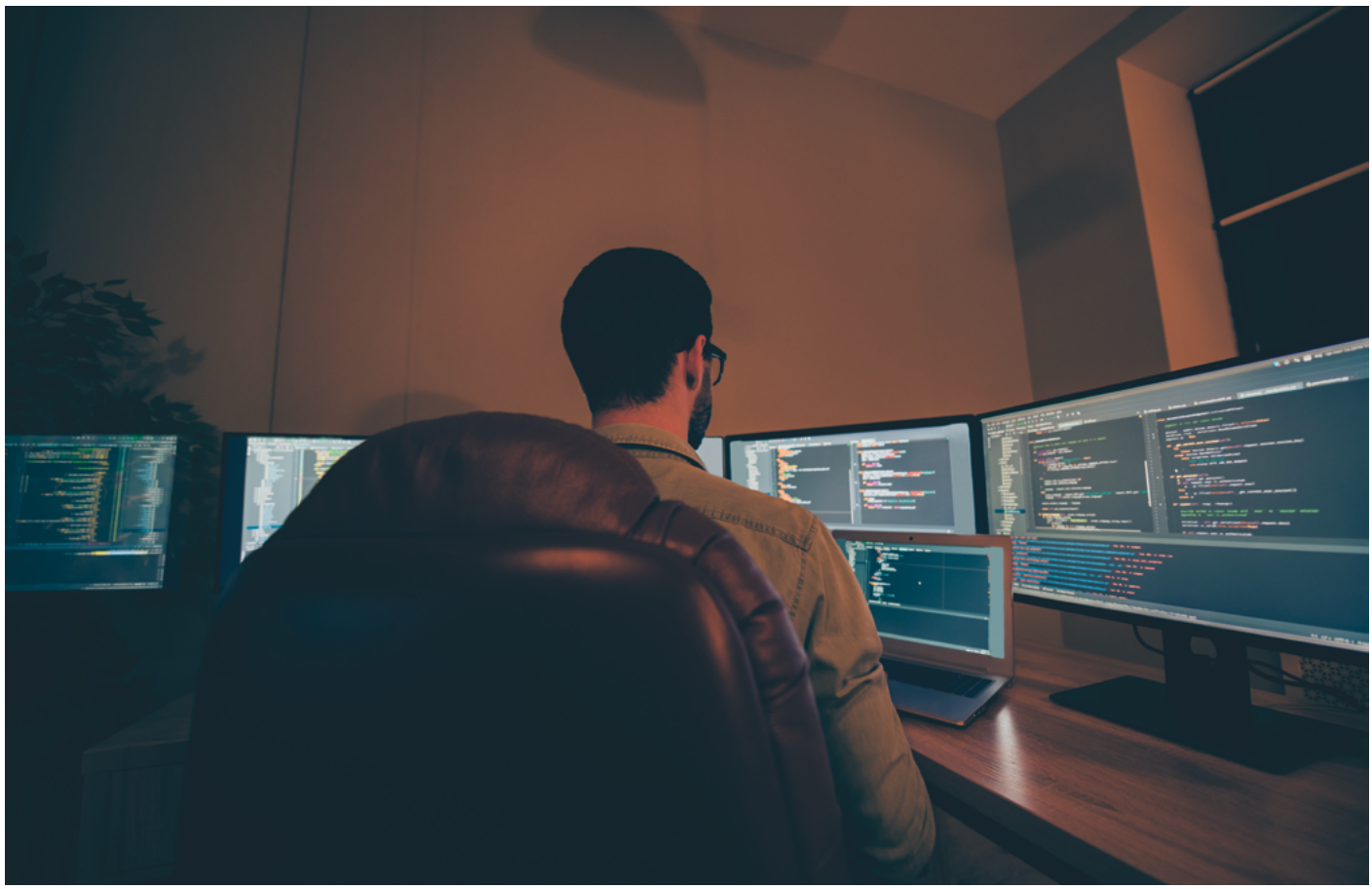
Un coup de projecteur sur la face cachée du piratage informatique est apporté par une récente affaire, qui s'est soldée par une faillite d'entreprise française et a conduit au chômage la majorité de ses employés, c'est-à-dire près de soixante au moment de sa liquidation judiciaire. Un matin de 2014, les informaticiens de cette PME intervenant dans le marketing direct constatent une intrusion sur son système d'information, avec copie frauduleuse de volumineux fichiers de données nominatives confiés par un gros client pour exécution d'une tâche (quoique la liste des OIV – opérateurs d'importance vitale – ne soit pas publique, ce client sera désigné ici par ce titre). Elle porte plainte et prévient ce client, lequel en informe sa propre clientèle, dans un effet boule de neige qui médiatise l'affaire, au-delà peut-on penser de ce que justifierait la valeur intrinsèque des données seulement constituées de noms et adresses. Appliquant sa politique de sécurité de manière draconienne, l'OIV engage la rupture du contrat de prestation qui le lie à la PME, perte majeure pour cette dernière, ajoutée à l'impact de notoriété contre son image de marque, qui l'asphyxie commercialement et la mène irrémédiablement au dépôt de bilan.

Une enquête rondement menée

Une enquête de police consécutive au dépôt de plainte a abouti, résultat rare et précieux, à identifier un auteur de l'attaque, situé en France également, en la personne d'un cadre d'une société – filiale d'un grand groupe étranger – par ailleurs concurrente de l'entreprise piratée, notamment lors d'un appel d'offres en cours. Lequel cadre a reconnu les faits, plaidé coupable selon la récente procédure inscrite dans le droit français de « comparution sur reconnaissance préalable de culpabilité » et a été condamné, mais lui sans guère de publicité faute de procès public (par un paradoxe mortel pour l'innocent, la faille technique du piraté a été médiatisée *urbi et orbi*, tandis que la faute intentionnelle du pirate l'a peu été). L'employeur et l'employé affirmeront aux enquêteurs

REPÈRES

La focalisation sur des événements ostensibles, placés au centre de la scène, laisse en coulisses trois types d'attaque moins perceptibles. Tout d'abord elle minore l'activisme des très gros acteurs d'État en matière d'interception ou de pénétration informatique. De fait, il est plus aisé et moins détectable de passer à l'acte, pour qui est concepteur et vendeur de l'électronique ou des logiciels déployés chez les victimes. Considération qui replace les USA et la Chine dans le groupe de tête des suspects. Ensuite le décompte sous-estime-t-il l'espionnage informatique, infiniment plus discret par nature que le hameçonnage ou les rançongiciels dont la vocation est de prendre contact avec la victime. Enfin privilégie-t-elle de lointaines origines, mystérieuses et sulfureuses, certainement fourbes et cruelles, alors que l'Orient, qui certes abrite bien des pirates, sert aussi de pivot pour des attaques par rebond dont l'origine nous est parfois voisine (concurrent, ancien employé…). Addition de ces deux dernières faces, l'espionnage de proximité s'en trouve gommé, pas vu pas pris, pas tracé pas localisé ; et avec lui ses préjudices.



© deagreez

qu'il s'agit d'une initiative spontanée du second ; point qui demeure l'objet d'interrogations, puisqu'il tend à exonérer le premier de certaines conséquences juridiques de tels actes.

Quelle est la qualification des faits ?

La qualification des faits s'entend non pas d'un seul point de vue juridique mais également d'un point de vue économique et éthique. Étrangement la justice a retenu à décharge le fait que les données copiées n'avaient pas été utilisées par le pirate, pour atténuer la sanction encourue. Étrangeté car, d'une part, cette inutilisation n'a pu s'apprécier que sur le laps de temps tronqué qui sépare le délit et l'interpellation par la police ; d'autre part le premier préjudice ne réside pas dans l'usage ou non de données volées, mais dans la potentialité de cet usage, qui oblige la victime à se comporter en fonction de cette hypothèse la pire, c'est-à-dire ici prévenir sa clientèle de la perte de confidentialité de leurs données donc se porter gravement tort en matière d'image et de réputation. Le tort résulte du vol en soi, même sans usage. Il y aurait d'autre part, venant d'un voleur de données, beaucoup de naïveté à utiliser commercialement et sous sa marque des fichiers d'adresses après s'en être emparé. Sans nécessité d'utiliser sous son identité de telles données, le copieur de fichiers détient de la dynamite en ce qu'il se trouve en mesure de faire savoir anonymement à l'OIV les faiblesses informatiques de son sous-traitant au cas où celui-ci omettrait de le prévenir du piratage (et de dévoiler en outre l'existence d'une telle rétention d'information), puis de la révéler aux clients de l'OIV si ce dernier oubliait de les prévenir. Ce qu'il a capté devient une arme, dont la puissance obligera A à informer B, puis B à informer C : le piratage, par sa seule perpétration, déclenche une mécanique infernale capable de ruiner la réputation informatique du piraté. Tout autant, à l'heure du *big data*, du KYC (l'art de connaître sa clientèle au-delà souvent de ce qu'elle croit) et de l'intelligence artificielle, disposer de fichiers de centaines de milliers de clients, même sans en faire de manière active un outil de démarchage, procure des informations de premier choix pour préparer du géomarketing ou mener des analyses sur la qualité de ces données, et aider à mieux profiler à la fois celui qui a fabriqué cette base de données et ceux qui s'y trouvent cités.

La duplication d'un fichier est-elle un vol ?

À un niveau plus conceptuel, la justice s'est longtemps partagée sur la question de savoir s'il y avait ou non vol, s'agissant de données informatiques qui n'ont pas été soustraites mais dupliquées. Or un parallèle simple existe avec une caméra cachée qui photographierait tel plan confidentiel de réacteur, comportement caractéristique de ce que l'homme de la rue qualifiera d'espionnage →

industriel plutôt que de vol, *a fortiori* si la commission de l'acte est renforcée par le statut de l'auteur, à savoir un concurrent. Différente est la jurisprudence dite *Bluetouff* en 2015, qui certes a vu la Cour de cassation consacrer la notion de vol de fichier informatique lorsqu'il y a copie même sans destruction, effectuée subrepticement sur le système d'information d'autrui, mais où l'accusé relevait d'un profil assez proche d'un lanceur d'alerte sur des dossiers de santé publique, et non pas de celui d'un concurrent. Le droit américain a accru, notamment depuis l'*Economic Espionage Act* de 1996, sa prédisposition à mettre en application l'accusation d'espionnage ou de concurrence déloyale. Il l'a fait à outrance et s'en sert comme d'un levier géopolitique ; *a contrario* la pugnacité américaine révèle la timidité de nos propres dispositions, avec un code pénal hésitant à reconnaître cette notion d'espionnage industriel.

L'intérêt de la présente affaire est de dépasser le stade des interrogations sur une éventuelle qualification d'espionnage industriel – l'acte en soi –, car elle aide à mesurer les conséquences d'un tel acte et à réfléchir au degré de causalité : la conséquence a-t-elle été fortuite ? Ici la victime disposait des moyens de protection normaux permettant de détecter l'intrusion advenue, à la suite de quoi elle ne pouvait pas, déontologiquement voire juridiquement, s'abstraire d'informer son client OIV, information qui a précipité quasi mécaniquement la perte d'un contrat vital, puis sa faillite. Les rouages, une fois engrenés, ont fait suivre à l'événement un parcours logique. Jusqu'à quel point un pirate peut-il invoquer l'imprévisibilité de cette cascade de conséquences, dès lors qu'elles entraient dans le champ des possibles, et de surcroît par un scénario d'une plausibilité suffisante pour en appeler à son éthique personnelle ? L'unique maillon de cet enchaînement tout à fait inhabituel au regard des statistiques judiciaires a été l'identification de l'auteur, œuvre de policiers spécialisés.

Quel recensement des dommages ?

Toujours par référence aux États-Unis, l'*Advocacy Center*, instance chargée de recevoir les doléances de leurs entreprises pour ce qu'elles considèrent être des agissements de concurrence déloyale étrangère, a eu dès ses origines l'habitude de publier un rapport annuel indiquant le nombre d'emplois et de contrats commerciaux sauvés par le soutien apporté aux plaignants. Or pareil bilan mais ici de non-assistance enregistrerait au contraire une entreprise défunte, plus d'une centaine d'emplois disparus (en comptant les emplois induits) avec une déperdition du savoir-faire industriel, des taxes que ne percevront plus les collectivités locales, donc des coupes budgétaires. Au-delà de ce premier recensement apparaît le fait que l'entreprise morte finançait à cette époque des innovations et un programme de R & D – soutenus par un fonds d'investissement régional – dans le domaine du numérique, aptes à faire franchir un saut qualitatif à son portefeuille de services. Un autre seuil franchi, mais à la baisse, tient à l'aggravation de fragilité de l'écosystème local, en l'occurrence un bassin d'emploi déjà touché par la désindustrialisation et où l'entreprise piratée faisait jusqu'alors figure d'espoir. Un pirate peut-il s'exonérer des conséquences socio-économiques de son acte, lorsqu'elles sont envisageables *ex ante* ?

"Le piratage, par sa seule perpétration, déclenche une mécanique infernale."

Et l'éthique, dans tout ça ?

De l'éthique personnelle à celle d'un collectif, il serait à demander à l'entreprise multinationale ayant déclaré avoir tout ignoré du piratage, pourtant mené par un de ses cadres, si tout au moins l'ambiance interne et l'atteinte des objectifs commerciaux attendue de son personnel n'ont pas primé dans les esprits sur des considérations de vertu. Un tel sujet dépasse la querelle de savoir si elle se considère juridiquement coupable, puisqu'elle clame l'ignorance, mais il oblige à se demander si elle s'estime moralement et pécuniairement impliquée par les conséquences sociales de ce qui a été commis par un de ses salariés contre un de ses concurrents. Se considère-t-elle victime elle aussi de son employé ? Et à qui doivent incomber les torts à réparer, le coût des chômeurs, les manques à gagner pour les collectivités locales, la perte pour les investisseurs ?

Enfin, la liste des victimes s'allonge encore car le savoir-faire déployé par le pirate n'est guère déconnectable de sa formation d'origine, en l'occurrence ingénieur d'une école qui nous est chère, puis d'une école d'application qui ne l'est pas moins. Cette collégialité souffre un peu, sourira-t-on, de ce que ce pirate ait été maladroit ou mauvais élève en informatique au point de mener à lui les policiers, mais elle souffre bien davantage de ce que le ciment commun bâti autour d'une éthique deux fois centenaire subisse de telles lézardes.

Pareille situation mène à demander si les cursus d'informatique dans l'enseignement supérieur pourront demeurer sans leur nécessaire pendant éthique et juridique : l'emploi fait de cet outil susceptible de devenir une arme contre autrui est aussi affaire de citoyenneté. Arme, car un simple ordinateur se montre capable, à coût infime, de provoquer des préjudices sans commune mesure, en tout lieu sur la planète. Rarement dans l'histoire la capacité à nuire à la liberté, à l'intégrité, à l'intimité ou à la réputation de nos contemporains n'a été portée à un point aussi élevé, par des équipements dont l'ingénieur est souvent concepteur ou utilisateur, dès lors confronté à ses responsabilités et à sa propre morale. La disproportion entre le moyen numérique et sa conséquence possible mériterait d'être enseignée et réfléchie. ×