Cour de cassation

chambre criminelle

Audience publique du 27 octobre 2009

N° de pourvoi: 09-82346

Publié au bulletin

REPUBLIQUE FRANCAISE

AU NOM DU PEUPLE FRANCAIS

LA COUR DE CASSATION, CHAMBRE CRIMINELLE, a rendu l'arrêt suivant :

Statuant sur le pourvoi formé par : - X...,
contre l'arrêt de la cour d'appel de MONTPELLIER, chambre correctionnelle, en date du 12 mars 2009,

qui, pour mise à disposition, sans motif légitime, de moyens conçus ou spécialement adaptés pour commettre une atteinte à un système de traitement automatisé de données, l'a condamné à 1000 euros d'amende ;

Vu le mémoire produit ;
Sur le moyen unique de cassation, pris de la violation des articles 8 de la Déclaration des droits de l'homme, 6 et 7 de la Convention européenne des droits de l'homme, [*l'article*] 6 de la Convention européenne sur la cybercriminalité du 23 novembre 2001, 34 et 37 de la Constitution, 323-1, 323-2, 323-3 et [*l'article*] 323-3-1 du code pénal, 111-3 et 121-3 du code pénal, 591 et 593 du code de procédure pénale, défaut de motifs et manque de base légale ;

"en ce que l'arrêt infirmatif [*de la cour d'appel de Montpellier*] attaqué a déclaré X... coupable de mise à disposition sans motif légitime de programmes ou données conçus ou adaptés pour une atteinte au fonctionnement d'un système de traitement automatisé de données, et, en répression, l'a condamné à une peine d'amende de 1 000 euros ;
"aux motifs que

le tribunal [*de première instance*] a relaxé X... au motif qu'il est établi que le site www n'incitait en aucune façon à l'utilisation de ces codes à des fins malveillantes ou de piratage informatique ; que la seule intention qui ait animé X... est un souci d'information des menaces existantes non corrigées à destination des utilisateurs de programmes

informatiques ; qu'il justifie d'ailleurs en avoir été remercié par Microsoft ; qu'aucune intention n'est établie ;

que [*toutefois*] **l'article 323-3-1 du code pénal [** *créé par la LCEN article 46* **] réprime 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 des atteintes aux systèmes de traitement automatisé des données, sans que le texte n'exige que soit caractérisée une incitation à l'utilisation d'un tel système** ;

que, s'agissant du motif légitime exonératoire, la cour estime que X... ne peut valablement arguer d'un motif légitime tiré de la volonté d'information dès lors que, par la mise en place d'un système de veille destiné à des abonnés et par la communication d'informations d'alerte directement à Microsoft à son adresse email, X... a fait la preuve de ce qu'il connaissait les dispositifs permettant de concilier le souci d'information avec la nécessaire confidentialité de ce type d'informations, étant précisé que X..., selon ses propres déclarations, n'a pas été remercié par Microsoft pour avoir publié sur le site web les exploits le concernant mais pour l'avoir avisé directement à son adresse mail des failles existantes ;

que, s'agissant de l'élément intentionnel de l'infraction, X... ne peut arguer de sa bonne foi alors que la fréquentation de son site par un public tout venant lui procurait des revenus publicitaires adossés au nombre de visiteurs ; qu'en conséquence, il est établi qu'il avait un intérêt économique à la diffusion d'informations dont il ne pouvait ignorer, du fait de son expertise en cette matière et ses antécédents judiciaires, qu'elles présentaient un risque d'utilisation à des fins de piratage par un public particulier en recherche de ce type de déviance ; qu'il y a lieu, en conséquence, d'infirmer le jugement déféré et de déclarer X... coupable de l'infraction poursuivie ; que, sur la peine, la cour constate que X... a développé son activité de conseil en matière de sécurité informatique ; qu'eu égard à sa personnalité et à sa progression professionnelle, il y a lieu d'être modéré dans la répression et de le condamner à une peine d'amende de 1 000 euros ;

"1°) alors qu'il n'y a point de délit sans intention de le commettre ;
que toute infraction doit être définie en des termes clairs et précis pour exclure l'arbitraire et permettre au prévenu de connaître exactement la nature et la cause de l'accusation portée contre lui ;
que
la Convention européenne sur la cybercriminalité réprime en son article 6, d'une part, la production, la vente, l'obtention pour utilisation, l'importation, **la diffusion ou d'autres formes de mise à disposition, soit d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre** la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus, soit d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant **d'accéder à tout ou partie d'un système informatique**, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5, et, d'autre part, la possession d'un élément visé aux paragraphes ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5 ;
qu'elle ajoute que cet article ne saurait être interprété comme imposant une responsabilité

pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique ;
qu'en s'en référant, pour retenir la culpabilité de X..., à l'article 323-3-1 du code pénal dont les termes généraux établissent une responsabilité pénale en l'absence de toute intention frauduleuse, la cour d'appel n'a pas légalement justifié la condamnation prononcée ;
"2°) alors qu'il n'y a point de délit sans intention de le commettre ; qu'en ne caractérisant pas de la part de X... une intention spécifique de diffuser les informations litigieuses dans le but précis de permettre la commission de l'une ou l'autre des infractions visées aux articles 323-1 à 323-3 du code pénal, la cour d'appel a privé sa décision de base légale au regard des textes susvisés ;
"3°) alors que, en se bornant, pour caractériser l'élément intentionnel de l'infraction reprochée à X..., à s'en référer à son intérêt économique et à considérer que les informations diffusées sur son site présentaient un risque d'utilisation à des fins de piratage, sans rechercher, ne serait-ce que pour écarter cette éventualité, si, nonobstant la conscience qu'il avait de l'existence d'un tel risque, X... n'avait pas été seulement animé de l'intention de remédier à une insécurité informatique, la cour d'appel a privé sa décision de base légale au regard des textes susvisés ;
"4°) alors que, de surcroît, en s'en référant, pour caractériser l'élément intentionnel de l'infraction, aux antécédents judiciaires de X..., sans mieux s'expliquer sur ce point au regard des circonstances de l'espèce, la cour d'appel, qui a statué par des motifs abstraits et généraux, a privé sa décision de base légale au regard des textes susvisés" ;
Attendu qu'il résulte de l'arrêt attaqué et des pièces de procédure que X... a diffusé sur le portail internet de la société XX Consulting, spécialisé dans le conseil en sécurité informatique, dont il est le gérant, des écrits directement visibles sur le site et accessibles à tous permettant d'exploiter des failles de sécurité informatique ; que, renvoyé devant le tribunal correctionnel pour mise à disposition, sans motif légitime, de moyens conçus ou spécialement adaptés pour commettre une atteinte à un système de traitement automatisé de données, il a été relaxé ;
Attendu que, pour infirmer, sur appel du ministère public, le jugement et condamner le prévenu, l'arrêt énonce qu'il ne peut valablement arguer d'un motif légitime tiré de la volonté d'information, dès lors que, du fait de son expertise en la matière, il savait qu'il diffusait des informations présentant un risque d'utilisation à des fins de piratage par un public particulier en recherche de ce type de déviance ;

Attendu qu'en l'état de ces énonciations, abstraction faite du motif surabondant relatif aux antécédents judiciaires du prévenu, et dès lors **que la constatation de la violation, sans motif légitime et en connaissance de cause, de l'une des interdictions prévues par l'article 323-3-1 du code pénal implique de la part de son auteur l'intention coupable** exigée par l'article 121-3 du même code,

la cour d'appel a justifié sa décision ;
D'où il suit que le moyen doit être écarté ;
Et attendu que l'arrêt est régulier en la forme ;

REJETTE le pourvoi ;

Ainsi jugé et prononcé par la Cour de cassation, chambre criminelle, en son audience publique, les jour, mois et an que dessus ;

Publication :

Décision attaquée : Cour d'appel de Montpellier du 12 mars 2009

Titrages et résumés : INFORMATIQUE - Données - Atteinte aux systèmes de traitement automatisé de données - Eléments constitutifs - Mise à disposition, sans motif légitime, de moyens conçus ou spécialement adaptés pour commettre une atteinte à un système de traitement automatisé de données

La constatation qu'il a agi sans motif légitime et en connaissance de cause établit l'intention coupable de celui qui, en violation de l'article 323-3-1 du code pénal, importe, détient, offre, cède ou met à disposition un moyen ou une information conçu ou spécialement adapté pour commettre une infraction d'atteinte aux systèmes de traitement automatisé de données. Justifie sa décision la cour d'appel qui retient qu'un prévenu ne pouvait arguer d'un motif légitime tiré de la volonté d'information dès lors que, du fait de son expertise, il savait qu'il diffusait des informations présentant un risque d'utilisation à des fins de piratage

FICHIERS ET LIBERTES PUBLIQUES - Informatique - Données - Atteinte aux systèmes de traitement automatisé de données - Eléments constitutifs - Mise à disposition, sans motif légitime, de moyens conçus ou spécialement adaptés pour commettre une atteinte à un système de traitement automatisé de données

Textes appliqués :
articles 121-3 et 323-3-1 du code pénal