VD_OMNI GE.2020.0217 vom 30. März 2021

VD Tribunal cantonal, 2021-03-30, FR

Quelle: https://mcp.opencaselaw.ch/entscheid/vd_omni_GE.2020.0217

FR: VD_OMNI GE.2020.0217 du 30 mars 2021

IT: VD_OMNI GE.2020.0217 del 30 marzo 2021

Regeste

A._____/Direction générale du numérique et des systèmes d'information - DGNSI, Préposé à la protection des données et à l'information | Recours d'un administré contre une décision de la DGNSI lui refusant l'accès à un document portant sur les vulnérabilités de l'application informatique ACTIS respectivement les moyens d'exploiter ces vulnérabilités et d'y remédier. La communication de ce document serait susceptible, à tout le moins, de compromettre la sécurité ou l'ordre publics, y compris s'agissant des vulnérabilités auxquelles l'autorité considère (à tort ou à raison) avoir remédié; un intérêt public prépondérant s'oppose ainsi à sa diffusion (consid. 2f). Le document concerné ne porte que sur des questions de sécurité informatique, de sorte que le recourant ne pourrait tirer aucune information d'une version de ce document dans laquelle ces éléments auraient été masqués (consid. 2g). Rejet du recours et confirmation de la décision attaquée. Recours au TF rejeté dans la mesure de sa recevabilité (arrêt 1C_235/2021 du 17 mars 2022).

Erwägungen

E. 1

Aux termes de l'art. 41 Cst-VD, l'Etat et les communes informent la population de leurs activités selon le principe de la transparence. Ce devoir d'information est réglementé dans la loi vaudoise du 24 septembre 2002 sur l'information (LInfo; BLV 170.21), qui s'applique notamment au Conseil d'Etat et à son administration, à l'exclusion de ses fonctions juridictionnelles (art.

E. 2

let. b LInfo). Cette exception peut être invoquée si deux conditions sont réalisées: les documents doivent concerner la sécurité ou l'ordre publics, d'une part, et leur communication doit présenter un risque de mise en danger de la sécurité ou de l'ordre publics, d'autre part (cf. Bastien von Wyss, Droit d'accès aux documents officiels: comparaison et étude de la mise en œuvre de quatre lois sur la transparence en Suisse, Mémoire de Master 2011, p. 47). e) Dans l'arrêt GE.2019.0010 précité (auquel l'autorité intimée se réfère dans sa réponse au recours), la cour de céans a eu l'occasion de se prononcer sur le bien-fondé d'une décision du Département des infrastructures et des ressources humaines (DIRH) refusant notamment au recourant l'accès à un document intitulé " Actis COPIL du 23 mai 2017 " (qualifié de " procès-verbal de la séance du 23 mai 2017 du COPIL ACTIS " par les parties), savoir une présentation sous forme de diapositives visant à assurer un suivi du développement de la plateforme ACTIS (cf. consid. 3b de cet arrêt). L'autorité intimée avait justifié son refus par le fait que la diffusion de ce document était susceptible de déboucher sur une intrusion malveillante ou un détournement de l'utilisation informatique ACTIS, soit sur un piratage, invoquant dans ce cadre - comme dans le cas d'espèce (cf. let. B supra) - une atteinte aux intérêts publics prépondérants

mentionnés à l'art. 16 al. 1 (recte : al. 2) let. a, b et d LInfo; le tribunal a retenu en particulier ce qui suit à ce propos (cf. consid. 4b de cet arrêt): "bb) Il est notoire que les logiciels informatiques comportent inévitablement des points faibles, des vulnérabilités, qui pourraient être exploitées par une personne malintentionnée pour empêcher l'utilisation du logiciel conformément à son but ou pour utiliser le logiciel à des fins non conformes à son but. Le recourant […] part […] du principe qu'il n'y a plus d'intérêt public prépondérant au secret lorsque les vulnérabilités découvertes ont été comblées. Cette approche est erronée. Il y a au contraire un intérêt public prépondérant à ce que les vulnérabilités d'un logiciel informatique utilisé par l'administration ne soient pas communiquées à l'extérieur. Il n'importe pas que l'autorité ait considéré à raison ou à tort que la vulnérabilité a été comblée. En effet, l'information du public sur des vulnérabilités apparemment comblées peut indiquer à un tiers malintentionné une zone sensible d'un logiciel et faciliter l'exploitation d'une vulnérabilité insuffisamment comblée ou d'une autre vulnérabilité annexe. Demeure réservée l'hypothèse dans laquelle les vulnérabilités d'un logiciel seraient susceptibles d'être la cause d'une atteinte aux droits fondamentaux ou aux droits politiques de la personne demandant accès. Le recourant ne soutient toutefois pas que tel serait le cas de la plateforme ACTIS. […] dd) Au vu de ce qui précède, c'est à juste titre que l'autorité intimée a estimé qu'il y a [vait] un intérêt public prépondérant s'opposant à la communication des vulnérabilités du logiciel ACTIS présentées dans le procès-verbal de la séance du 23 mai 2017 du COPIL ACTIS." f) En l'espèce, l'autorité intimée a exposé en particulier ce qui suit pour justifier son refus de communiquer le document en cause au recourant dans sa réponse au recours: "f) Le test d'intrusion - ACTIS, B._____ sàrl, 2017 […] est un rapport de tests de sécurité sous la forme de diapositives PowerPoint, produit par la société B._____ sàrl, spécialisée dans la sécurité des systèmes d'information. Ce type de rapport met en exergue les éventuelles vulnérabilités d'un système informatique et explique les manières d'exploiter ces failles et par conséquent les actions adéquates pour y remédier. […] g) […] le test d'intrusion - ACTIS [,] B._____ sàrl, 2017 fait état des vulnérabilités concrètes et des correctifs nécessaires à la sécurité informatique non seulement de la plateforme ACTIS, mais également d'autres applications et systèmes connexes de l'Etat de Vaud. […] h) […] ces vulnérabilités ne doivent en aucun cas être divulguées à des tiers, car il s'en suivrait un risque accru de piratage de l'application et des systèmes connexes. […] Un piratage d'ACTIS et d'autres systèmes connexes serait dommageable en ce qui concerne l'intégrité, la confidentialité et la traçabilité des données qui transitent par ces systèmes. Un hacker, même doté d'une expérience limitée, serait en mesure d'orienter ses actions de manière à porter préjudice à la plateforme ACTIS et aux autres systèmes connexes concernés en suivant les précisions inclues dans le rapport et la manière d'exploiter les failles découvertes. Il pourrait ainsi compromettre l'application, prendre la maîtrise d'un serveur (ce qui lui permettrait d'agir également sur d'autres serveurs) ainsi qu'injecter des données dans les systèmes ou en extraire massivement. Pour toutes ces raisons, donner accès à ces informations présente le risque que les procédures de permis de construire et plus généralement la sécurité des systèmes concernés soient considérablement exposées à un acte malveillant et dommageable. i) […] les systèmes d'information ne fonctionnent pas en silos cloisonnés, ils sont au contraire bien souvent interconnectés, de telle sorte que les vulnérabilités et failles détectées lors d'un test d'intrusion ne concernent que rarement une seule application ou un seul système, renforçant ainsi le caractère déjà très sensible des informations contenues dans un rapport de sécurité tel que celui qui est objet de la présente procédure. j) De manière générale, même le

personnel de la [DGNSI] n'est pas mis au courant des problèmes touchant la sécurité d'une application, cela pour éviter des risques de fuite d'informations sensibles vers l'extérieur. Il s'agit de mesures de protection standards appliquées à l'ensemble de l'Administration cantonale vaudoise dans le domaine de l'informatique. Compte tenu de leur haute sensibilité, l'accès à ces rapports de sécurité est très restreint et fait l'objet d'une protection stricte, leur dossier de stockage étant par ailleurs chiffré. k) Contrairement ce qu'allègue le recourant, les problèmes de sécurité de la plateforme ACTIS ne sont pour l'heure pas encore entièrement résolus. De fait, les vulnérabilités constatées concernent également des systèmes et applications connexes, ce qui complexifie leur traitement. Les délais fixés dans la planification des correctifs n'ont malheureusement pas pu tous être respectés. […] " Ces explications entraînent la pleine conviction du tribunal quant à la vraisemblance du risque sérieux et actuel que représenterait la communication du rapport au cause en tant qu'une telle communication serait susceptible, à tout le moins, de compromettre la sécurité ou l'ordre publics au sens de l'art. 16 al. 2 let. b LInfo. Les conséquences que pourrait avoir une intrusion malveillante et le fait que les systèmes d'information vaudois sont dans une large mesure interconnectés (cf. let. h et i), en particulier, obligent dans ce cadre à retenir que le dommage pour la sécurité et l'ordre publics serait suffisamment grave et exceptionnel pour justifier la non-diffusion de ce document (cf. consid. 2 d supra). Il n'y a en outre pas lieu, quoi qu'en pense le recourant, de distinguer entre les vulnérabilités relevées dans ce rapport auxquelles il aurait d'ores et déjà été remédié et les problèmes de sécurité qui n'auraient pas encore été entièrement résolus; on peut se référer à cet égard à la teneur du consid. 4b/bb de l'arrêt GE.2019.0010 précité, en ce sens en substance que l'information du public quant à l'existence d'une vulnérabilité est susceptible de présenter des risques même dans l'hypothèse où l'autorité a considéré, à tort ou à raison, qu'il y avait été remédié (cf. consid. 2e supra); compte tenu des enjeux, on ne saurait faire grief à l'autorité intimée de faire montre d'une prudence particulière en la matière. g) Le recourant soutient par ailleurs que l'autorité intimée aurait néanmoins dû répondre au moins partiellement à sa demande, en masquant le cas échéant les informations susceptibles d'entraîner un risque sécuritaire. L'art. 17 LInfo prévoit en effet, en substance, que le refus de communication d'un document pour un motif d'intérêt public ou privé prépondérant ne vaut que pour la partie de ce document concerné par l'intérêt en cause respectivement que l'autorité doit s'efforcer de répondre au moins partiellement à la demande. Dans l'arrêt GE.2019.0010 précité, le tribunal a ainsi retenu que le document en cause contenait également d'autres informations que celles relatives à des vulnérabilités connues à cette date de l'application concernée (données financières et de ressources humaines, données statistiques, échéanciers et planning) et que " seules p [ouvaient] être soustraites au droit à l'information les informations protégées par l'intérêt public prépondérant pertinent, à savoir en l'espèce l'intérêt public à ce que les vulnérabilités d'un logiciel informatique utilisé par l'administration ne soient pas communiquées à l'extérieur " (cf. consid. 5a de cet arrêt); il a en conséquence réformé la décision attaquée en ce sens que le document serait remis au recourant dans une version caviardée, excluant les informations liées aux problèmes de sécurité (cf. consid. 5b de cet arrêt). En l'occurrence toutefois, le rapport intitulé " Test d'intrusion - ACTIS " établi en 2017 par la société B._____ Sàrl porte exclusivement sur les vulnérabilités de ce système informatique et sur les manières d'exploiter ces failles et des actions pour y remédier, qui sont directement liées. Le recourant ne pourrait en conséquence tirer aucune information d'une version de ce document dans laquelle ces éléments auraient été masqués. Dans ces conditions, la décision attaquée ne prête pas le flanc à la critique.

E. 3

Il résulte des considérants qui précèdent que le recours doit être rejeté et la décision attaquée confirmée. Il n'est pas perçu d'émolument (cf. art. 49 al. 1 LPA-VD et 27 al. 1 LInfo) ni alloué de dépens (cf. art. 55 al. 1 LPA-VD).