

VD_OMNI GE.2025.0054 vom 16. Juni 2025

VD Tribunal cantonal, 2025-06-16, FR

Quelle: https://mcp.opencaselaw.ch/entscheid/vd_omni_GE.2025.0054

FR: VD_OMNI GE.2025.0054 du 16 juin 2025

IT: VD_OMNI GE.2025.0054 del 16 giugno 2025

Regeste

A. _____ /Municipalité de Vevey | Refus d'une municipalité de communiquer des informations sur une cyberattaque subie. Pesée des intérêts (art. 16 al. 1 LInfo): l'intérêt public à la confidentialité du traitement de la cyberattaque l'emporte sur celui à la diffusion des informations qui s'y rapportent. Recours rejeté.

Erwägungen

E. 1

a) A teneur de l'art. 26 LInfo, les autorités communales statuent sur les demandes concernant leurs activités; elles le font par le biais de décisions. L'art. 24 LInfo prévoit, à son al.1, que la procédure de recours devant le Tribunal cantonal est rapide, simple et gratuite. Quant à son al. 3, il prévoit que la loi vaudoise du 28 octobre 2008 sur la procédure administrative (LPA-VD; BLV 173.36) est applicable aux décisions rendues en vertu de la présente loi, ainsi qu'aux recours contre dites décisions. Il en découle que les décisions des municipalités, rendues en application de l'art. 26 LInfo sont susceptibles de recours à la CDAP (art. 92 LPA-VD). b) Le recourant, destinataire de la décision lui refusant l'accès au document demandé, auquel il prétend avoir droit, a la qualité pour recourir (art. 75 al. 1 let. a LPA-VD). Le recours a de plus été formé dans le délai (art. 95 LPA-VD) et le respect des formes prescrites (art. 79 et 99 LPA-VD). Il y a partant lieu d'entrer en matière. c) L'autorité intimée a formulé diverses réquisitions d'instruction. Compte tenu de l'issue du pourvoi, il n'y a pas lieu de donner suite à ces réquisitions.

E. 2

Des intérêts publics prépondérants sont en cause lorsque : a. la diffusion d'informations, de documents, de propositions, d'actes et de projets d'actes est susceptible de perturber sensiblement le processus de décision ou le fonctionnement des autorités; b. une information serait susceptible de compromettre la sécurité ou l'ordre publics; [...] d. les relations avec d'autres entités publiques seraient perturbées dans une mesure sensible. [...]" Selon l'art. 17 LInfo, le refus de communiquer un renseignement ou un document conformément à l'art. 16 ne vaut le cas échéant que pour la partie du renseignement ou du document concerné par cet article et tant que l'intérêt public ou privé prépondérant existe (al. 1); l'organisme sollicité s'efforce de répondre au moins partiellement à la demande, au besoin en ne communiquant pas ou en masquant les renseignements ou les parties d'un document concernés par l'intérêt public ou privé prépondérant (al. 2). d) D'une façon générale, l'art. 16 LInfo doit être interprété de façon similaire à l'art. 7 de la loi fédérale du 17 décembre 2004 sur la transparence (LTrans; RS 152.3). Le refus d'accès (total ou partiel) doit ainsi se justifier par un risque à la fois important et sérieux d'atteintes aux intérêts publics ou privés prépondérants protégés par cette disposition; l'application de ces exceptions, restrictive, doit résulter d'une pesée des intérêts et respecter le principe de la

proportionnalité. Le fardeau de la preuve pour réfuter la présomption de publicité établie par la LInfo est à la charge de l'autorité (CDAP GE.2019.0010 du 4 octobre 2019 consid. 4a et les références). S'agissant en particulier de l'hypothèse prévue par l'art. 16 al. 2 let. b LInfo en lien avec le risque de compromission de la sécurité ou de l'ordre publics, c'est dans chaque cas d'espèce que les autorités doivent déterminer si les conditions en sont réunies, étant précisé que ce motif doit rester l'exception et non pas se transformer en règle; le dommage pour la sécurité ou l'ordre publics doit ainsi être suffisamment grave et exceptionnel pour justifier la non-diffusion d'une information sous motif d'intérêt public prépondérant (cf. EMPL précité, p. 2656 ad art. 16 al. 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, 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) Dans le souci d'être complet, on ajoutera que le droit fédéral prévoit, depuis le 1^{er} avril 2025, une obligation d'annonce des cyber-attaques à charge des infrastructures critiques. aa) Le Parlement fédéral a en effet adopté, le 18 décembre 2020, la loi fédérale sur la sécurité de l'information au sein de la Confédération (ci-après: LSI; RS 128). A teneur de son art. 3, cette loi ne s'applique que de

manière limitée aux cantons (notamment lorsque ceux-ci accèdent à des moyens informatiques de la Confédération); elle s'applique en outre aux organisations de droit public ou privé qui exploitent des infrastructures critiques; si elles ne sont pas visées par l'art. 2 al. 1 à

E. 3

Il demeure que le présent litige concerne l'application de la LInfo et non un éventuel droit d'accès auprès des autorités fédérales fondé sur la LTrans. Il n'est d'ailleurs pas contesté que les activités de l'autorité intimée dans le domaine informatique (en l'occurrence la gestion du site de cette ville) entrent dans le champ d'application de la LInfo. Il demeure que, conformément à la systématique de cette loi, des exceptions à la transmission peuvent être opposées au requérant en présence d'intérêts prépondérants, publics ou privés. L'autorité requise doit ainsi procéder à une pesée d'intérêts entre l'intérêt public à la diffusion de l'information et les intérêts opposés, soit notamment l'existence d'un intérêt public au refus de renseigner. Cette pesée peut conduire à un refus pur et simple, à une remise partielle des documents (ou renseignements) demandés, voire à différer la transmission (art. 16 al. 1 et 17 LInfo).

a) aa) L'information relative à une cyber-attaque, en soi, présente un intérêt public, par exemple lorsque celle-ci entraîne des perturbations plus ou moins graves dans le fonctionnement de services publics. En outre, lorsque la cyber-attaque a pour conséquence des fuites de données personnelles, il y a un intérêt individuel, correspondant sans doute à un intérêt public également, à ce que les personnes concernées soient informées (sur ces points, voir notamment art. 73c et 73d LSI, qui s'appliquent désormais aux autorités communales).

bb) Toutefois, il convient de prendre en compte également, en sens contraire, un intérêt public à la confidentialité des données recueillies autour de cyber-attaques, et notamment des rapports et analyses effectués à ce propos. L'art. 4 al. 1bis LSI le prévoit d'ailleurs expressément. Cela étant, dans la mesure où cette disposition, entrée en vigueur le 1^{er} avril 2025 n'est de toute façon pas applicable par l'autorité intimée dans le cadre de la LInfo, force est pour cette dernière de procéder à une pesée d'intérêts, conformément à l'art. 16 al. 1 LInfo. On peut préciser à ce propos que l'intérêt public ici en cause a trait à la sécurité de l'information. Cependant, ce thème est appréhendé de manière différente en droit fédéral et en droit vaudois. La portée de ce principe est en effet précisée à l'art. 6 LSI et il couvre des exigences de confidentialité, de disponibilité, d'intégrité et de traçabilité (voir art. 6, spéc. al. 2 LSI). S'agissant du droit vaudois, ce principe est énoncé dans la loi vaudoise du 11 septembre 2007 sur la protection des données personnelles (LPrD; BLV 172.65); ainsi, à teneur de l'art. 10 LPrD, le responsable du traitement prend les mesures appropriées pour garantir la sécurité des fichiers et des données personnelles, soit notamment contre leurs pertes, leurs destructions, ainsi que tout traitement illicite. Cette disposition exprime ainsi surtout un intérêt public en lien avec la protection de données personnelles; autrement dit, l'intérêt public à la disponibilité des informations diffusées par un site, tel que celui de l'autorité intimée, n'est pas pris en compte à l'art. 10 LPrD – contrairement à ce qui prévaut dans le cadre de la LSI. Il n'en demeure pas moins que l'autorité intimée est tout à fait habilitée à prendre en compte cet aspect de disponibilité au titre de l'intérêt public dans la pesée des intérêts à laquelle elle procède dans le cadre de l'art. 16 al. 2 let. b LInfo.

cc) Il en découle que l'autorité intimée, lorsqu'elle a été saisie de la requête du recourant en lien avec la cyber-attaque de janvier 2025, était habilitée à donner à l'intérêt public à la confidentialité du traitement de la cyber-attaque en cause un poids prépondérant par rapport à l'intérêt public à la diffusion des informations qui s'y rapportaient. Ce faisant, l'autorité intimée ne faisait que suivre l'exemple adopté par le

législateur fédéral lui-même. dd) Il en découle que le recours, mal fondé dans son principe, doit être rejeté. b) Ce résultat de principe doit d'ailleurs être confirmé au regard des différents documents ou informations plus précises requises par le recourant (dans sa demande, précisée par son recours). En effet, on a vu que les réactions de l'autorité communale à la suite d'une cyber-attaque devaient être traitées de manière confidentielle; cela vaut pour le rapport technique décrivant la nature de l'attaque et son impact; il en va de même des mesures mises en place ou envisagées pour renforcer la sécurité informatique ou encore les éventuelles vulnérabilités créées par une migration vers un serveur géré par l'autorité intimée, à la suite de la reprise par l'entreprise C. _____ du mandat de gestion du site de la Ville. Enfin, la question du coût des actions correctives entreprises, qui ne sont sans doute pas encore achevées, pourra être traitée dans le cadre des comptes de la commune, à une date ultérieure, sans doute en 2026; en d'autres termes, la demande apparaît sur ce dernier point prématurée.

E. 4

Il découle des considérations qui précèdent que le recours doit être rejeté. Vu la gratuité de la procédure, le présent arrêt doit être rendu sans frais. En revanche, le recourant, qui succombe, doit verser une indemnité de dépens à la commune de Vevey (art. 27 LInfo et 55 LPA-VD).

Export aus OpenCaseLaw (CC0). Verbindlich ist allein der vom erlassenden Gericht veröffentlichte Originaltext. Quellen-URL siehe oben.