consumer protection as well as cybersecurity issues and data breach management.

Joe received a bachelor's degree in civil law from Université de Montréal in 2016 and a Bachelor's degree in Microbiology and Immunology from McGill University in 2013. He is currently completing a Master of Laws degree in Information Technology Law at Université de Montréal.]

---

1 [2017] S.C.J. No. 33, 2017 SCC 33, available at: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16700/index.do.

2 [2003] S.C.J. No. 23, [2003] 1 S.C.R. 450, available at: http://canlii.ca/t/1g5lx.

3 R.S.B.C. 1996, c. 373, available at: http://www.bclaws.ca/Recon/document/ID/freeside/00_96373_01.

4 R.S.N.L .1990 c. P-22, available at: http://assembly.nl.ca/Legislation/sr/statutes/p22.htm.

5 R.S.S. 1978, c. P-24, available at: http://canlii.ca/t/h7q9.

6 CQLR c. CCQ-1991, available at: http://legisquebec.gouv.qc.ca/en/showdoc/cs/CCQ-1991.

7 CQLR c. C-12, available at: http://legisquebec.gouv.qc.ca/en/showdoc/cs/C-12.

8 CQLR c. P-40.1, available at: http://legisquebec.gouv.qc.ca/en/showdoc/cs/P-40.1.

9 *St-Arnaud v. Facebook inc.*, [2011] Q.J. No. 3161, 2011 QCCS 1506, available at : http://canlii.ca/t/fkvmj.

• PROFESSIONALS TAKE HEED: A DECISION AT THE CROSSROADS OF DISCIPLINARY LAW AND CYBERSECURITY •

Antoine Guilmain, Associate, and Antoine Aylwin, Partner, Fasken Martineau DuMoulin LLP

Antoine Guilmain

Antoine Aylwin

On June 7, 2017, the disciplinary council of the Ordre des CRHA/CRIA[1] issued a fundamental decision that lies at the crossroads of professional and disciplinary law, the protection of privacy and information, and information technologies: *Conseillers en ressources humaines et en relations industrielles agréés (Ordre professionnel des)* c. *Milot*, 2017 CanLII 35570 (QC CDRHRI).

This decision essentially offers a number of lessons concerning the duty of professionals to be technologically competent, security measures to be applied when transmitting technological documents, and, more broadly, certain cybersecurity issues. This bulletin will therefore summarize (1) the facts to which the decision relates; (2) the positions of the parties; (3) the analysis by the disciplinary council; (4) the lessons to be learned in relation to professional and disciplinary law; and (5) the lessons to be

learned in terms of cybersecurity and information technologies.

SUMMARY OF THE FACTS

A disciplinary complaint was made against a person ("**Respondent**") who was a member of the Ordre des conseillers en ressources humaines et en relations industrielles agréés du Québec ("**Order**"). The individual was accused of failing to comply with her professional secrecy obligations by sending a copy of a confidential report from a psychiatrist concerning an employee to third parties, without authorization, contrary to sections 60.4 and 59.2 of the *Professional Code*[2] and section 51 of her *Code of Ethics*.[3]

On February 19, 2016, in the course of her occupational health and safety duties at an Integrated Health and Social Services Centre ("**CISSS**"), the Respondent received a psychiatric report concerning an employee. The facts of the case took place over a very short period of time:

> 10:26 a.m.: The Respondent sent an email to the employee concerned containing a notice to return to work based on that report, copying the message to the employee's superior and the president of the union;
>
> 10:29 a.m.: A second email was sent to the same recipients, because the Respondent had neglected to attach the psychiatric report;
>
> 3:00 p.m.: On being informed by the union president, the Respondent realized that the psychiatric report had been sent to the employee's superior without the employee's authorization. The Respondent tried to recall or destroy the email sent to the superior by computer, but was unable to do so. The Respondent then decided to call the employer's superior, who confirmed that he had destroyed the email without opening it and without seeing the content of the report attached to it.

POSITION OF THE PARTIES

The syndic argued that the Respondent had committed a serious breach of ethics by transmitting the report to the employee's superior and the president of the employee's union without authorization to do so. The report was, in fact, highly confidential in nature, and that lies at the heart of professional secrecy. The Complainant further argued that the Respondent had taken no measures to ensure that the secrecy of confidential information brought to her attention in the practice of her profession was preserved.

The Respondent, who was not represented by counsel, alleged that she had made an unfortunate mistake by transmitting the report to the employee's superior and the president of the employee's union. The Respondent further argued that she had *quickly* taken all appropriate steps to correct her mistake and contended that no prejudice had resulted for the employee.

ANALYSIS BY THE DISCIPLINARY COUNCIL

The council was required to answer the following question: did the mistake made by the Respondent constitute a breach of ethics? The council's ultimate answer was that it did, and it found the Respondent guilty on the disciplinary complaint relating to the violation of professional secrecy.

The council offered numerous arguments to justify its decision; those arguments are crucial in cases involving the use of information technologies, and we will come back to them. They can be summarized as follows:

- Importance of professional secrecy. The council first focused on professional secrecy and Quebec society and the importance of the secrecy of any confidential information in disciplinary law.
- "Confidential" notation on a document. The council then found that the psychiatric report contained several particularly sensitive pieces of medical information and stressed that the notation "confidential" on the cover page of the report "should have served as a reminder to the Respondent to take the greatest precautions."[4]
- Prevention by the Order. The council further noted that the Order cautions its members regarding "the risks inherent in the use of modern communication tools in the practice of their profession"[5] and that those tools "are poorly suited to the secure transmission of information that is confidential

or protected by professional secrecy".[6] The Order therefore urges its members to adopt, for example, one of the following protective measures: "encrypt confidential documents, assign them a password or access code to limit access, or use any other available security measure that is more likely to protect the confidentiality of the documents."[7]

- No contact with the IT department. In this case, the Respondent did not take any of those protective measures. Later in the decision, the council stated: "moreover, in the absence of evidence showing that she spoke with the CISSS' IT department … to obtain advice concerning the most suitable available security measures for ensuring that the confidentiality of information obtained in the course of her professional activities was preserved, the board has no choice but to find her guilty on the violation charged in the disciplinary complaint."[8]
- Proof of consent. The council further noted that there was no indication that the employee had consented to being contacted by email by the Respondent or persons authorized to access his file.
- Lack of attention. The council found that "the lack of attention cited by the Respondent confirms her failure to take appropriate measures to ensure that the secrecy of the confidential information … that was brought to her attention in the practice of her profession was preserved",[9] adding that "the mistake made by the Respondent indicates that she was careless with respect to her obligation to act in such a way as to ensure confidentiality".[10]
- Contractual obligations. The council believed that in addition to professional obligations, the Respondent was required to comply with the policies in force at the CISSS, which prescribe general and specific obligations concerning the confidentiality of information collected, including that it be protected by limiting access to authorized persons only.
- Two emails in succession. The council further found that "the Respondent [sent] an email to the two unauthorized persons the second time, and this should have been another opportunity for her to question the legitimacy of sharing the report with them",[11] that is, with the union president and the employee's superior.
- Standard clause at the bottom of emails. The council stressed that the standard "for intended recipients only" clause at the bottom of emails is "insufficient in proportion to the importance of the fundamental right [of professional secrecy] to be preserved",[12] did not allow the Respondent to "delegate to the recipients her professional responsibility to preserve the secrecy of confidential information that comes to her attention in the practice of her profession",[13] and "offers no guarantee that the confidential document will not be accessed".[14]
- Speed of the communications. The council found that the short time between when the mistake was made and the attempt to mitigate the damage (about five hours) was not "an acceptable justification to explain the failure by the Respondent to take appropriate measures to ensure the confidentiality of the report".[15] The council also reiterated the well-known maxim that confidentiality only lives once.
- Record. Whether the Respondent intended to violate the confidentiality of information protected by secrecy is not a relevant factor to be considered in disciplinary law. Accordingly, the council found the Respondent guilty under section 60.4 of the Professional Code, which imposes an obligation of professional secrecy on all professionals.

It must also be noted that the sanction is not yet known and a further hearing will be held to determine it. The type of sanction (reprimand, fine, striking off, etc.) should provide an even better indication of the seriousness of the offence charged and the repercussions for other professionals.

LESSONS IN RESPECT OF PROFESSIONAL LAW AND DISCIPLINARY LAW

This decision should not be regarded as isolated or unique to one professional order (here, CRHAs/CRIAs); quite the contrary. This is a strong signal to *all* professionals concerning their obligations in relation to information technologies.

The decision tells us that neither the accelerated speed of communications nor technological blunders is a valid defence (watch out for mistakes concerning recipients), that the standard "for intended recipients only" clause at the bottom of emails is not sufficient (in spite of how widespread its use is), to think twice before sending an email (or demonstrate negligence, otherwise), to maintain close and regular contact with the IT department, that contractual obligations concerning security must be read and incorporated into professionals' practices, that reasonable security measures must be taken, that proof of consent to electronic communication should be retained, and so on.

Obviously, most professional orders already make efforts to ensure that their members are aware of these issues, often by issuing directives (as the Ordre des CRHA/CRIA does) or an IT manual (as the Barreau du Québec does). However, while there are those who are not persuaded that the rules in question are enforceable, this decision will remind them that a member's conduct must nonetheless take them into account. In addition, there is the obligation of general competence, which, in our opinion, also covers the use of information technologies and issues in the protection of information.

This case points to the obligation of "technological competence" in the Codes of Ethics for which some bodies are campaigning. These include the Federation of Law Societies of Canada, which in January 2017 included a clause in its Model Code of Professional Conduct concerning technological competence that reads as follows: "To maintain the required level of competence, a lawyer should develop and maintain a facility with technology relevant to the nature and area of the lawyer's practice and responsibilities. A lawyer should understand the benefits and risks associated with relevant technology, recognizing the lawyer's duty to protect confidential information set out in section 3.3." The American Bar Association also advocates an evolution of the ethical rules with regard to information technology, in particular to the obligation of competence.

To summarize, this decision must be seen by *all* professionals as a first step toward an obligation of technological competence.

LESSONS IN RESPECT OF CYBERSECURITY AND INFORMATION TECHNOLOGIES

This decision also extends to the realm of information technologies. First, we can see numerous connections with the *Act to establish a Legal Framework for Information Technology*[16] ("**ALFIT**), particularly with respect to transmission of documents. While section 29 addresses the choice of medium, it is silent as to proof and retention of that choice; according to the decision, however, consent should be obtained each time before communicating by email. While the authors have their doubts and are reluctant to subscribe to the conclusion, it must be taken seriously by businesses, in particular. In addition, this decision further strengthens and clarifies section 34 ALFIT, which provides: "Where the information contained in a document is declared by law to be confidential, confidentiality must be protected by means appropriate to the mode of transmission, including on a communication network." We would note here that ALFIT was never cited in the decision.

Second, this decision also affects employers of professionals who are bound by professional secrecy. Internal policies regarding the security and confidentiality of information are binding on those professionals, who must comply with them in addition to their ethical obligations. Moreover, prevention in these matters is not solely the responsibility of the professional orders; it is also incumbent on professionals themselves, who must obtain training, ensure that they are aware of the issues, and stay up to date regarding the security and confidentiality of information.

Third, this decision provides concrete examples of security measures to take in order to protect personal information, whether by encryption, passwords, or access codes (see section 10 of the *Act respecting the Protection of Personal Information in the Private Sector*[17] or Principle 7 in Schedule 1 of

the *Personal Information Protection and Electronic Documents Act*[18]).

The purpose of this bulletin is to provide an initial overview of this decision, which is extremely comprehensive and is of particular interest not only to professionals, but also to all businesses and organizations that use electronic document transmission (in particular, email). In other words, everyone should feel that it concerns them!

[***Antoine Aylwin*** *is a partner at Fasken Martineau's Montreal office and a member of the Privacy and Information Protection Group. He regularly pleads before various judicial courts and administrative tribunals, and he is often asked to speak or write about privacy and information protection.*

Antoine Guilmain *is an associate at Fasken Martineau's Montreal office and a member of the Privacy and Information Protection Group. As such, he works in the areas of personal information protection, access to information, online advertising and marketing, cybersecurity, information technologies and intellectual property.*]

---

1 CRHA stands for "Conseillers en Ressources Humaines Agréés" [Certified Human Resources Professionals] and CRIA stands for "Conseillers en Relations Industrielles Agréés" [Certified Industrial Relations Counsellors].

2 CQLR c. C-26.

3 CQLR c. C-26, r 81.

4 Para. 70 [all quotations from the decision have been translated from the original French].

5 Para. 73.

6 Para. 74.

7 *Ibid.*

8 Para. 76.

9 Para. 83.

10 Para. 100.

11 Para. 89.

12 Para. 93.

13 Para. 94.

14 Para. 98.

15 Para. 103.

16 CQLR c. C-1.1.

17 CQLR c. P-39.1.

18 S.C. 2000, c. 5.