

[TRANSLATION]

Citation: PD v Canada Employment Insurance Commission, 2022 SST 481

# Social Security Tribunal of Canada General Division – Employment Insurance Section

# **Decision**

**Appellant:** P D.

Respondent: Canada Employment Insurance Commission

**Decision under appeal:** Canada Employment Insurance Commission

reconsideration decision (449878) dated January 27,

2022 (issued by Service Canada)

Tribunal member: Josée Langlois

Type of hearing: Videoconference Hearing date: April 13, 2022

Hearing participant: Appellant

**Decision date:** April 19, 2022 **File number:** GE-22-742

#### Decision

- [1] The appeal is dismissed.
- [2] The Appellant's actions are misconduct under the *Employment Insurance Act* (Act). This means that he is disqualified from receiving Employment Insurance (EI) benefits.<sup>1</sup>

#### **Overview**

- [3] The Appellant lost his job as a salesperson at Telus Mobile Inc. His employer says he was let go because he had his computer equipment shipped to another country and worked remotely in that country without authorization. The Appellant's actions went against the security rules he was supposed to follow. They also affected the work duties of other employees and many of the company's customers, since the system had to be shut down indefinitely.
- [4] The Appellant agrees he was let go for this reason. However, he says it was only after the system was shut down that he learned he wasn't allowed to have the employer's computer equipment shipped to Senegal. He also says he only did this to avoid losing his job since he had gotten COVID-19 and could not return to Canada.
- [5] The Commission accepted the employer's reason for the dismissal. It decided that the Appellant lost his job because of misconduct. Because of this, the Commission decided that the Claimant is disqualified from receiving EI benefits.

#### Issue

[6] Did the Appellant lose his job because of misconduct?

<sup>1</sup> Section 30 of the *Employment Insurance Act* (Act) says that claimants who lose their job because of misconduct are disqualified from receiving benefits.

## **Analysis**

[7] To answer the question of whether the Appellant lost his job because of misconduct, I have to decide two things. First, I have to determine why the Appellant lost his job. Then, I have to determine whether the Act considers that reason to be misconduct.

### Why did the Appellant lose his job?

- [8] I find that the Appellant lost his job because he didn't follow the employer's security rules on the use of computer equipment. The Appellant had another person ship computer equipment belonging to the employer to another country. He also used the SIM card from his employer-provided cell phone and his computer to work in that country without his employer's permission.
- [9] The Commission and the Appellant agree on why the Appellant lost his job.
- [10] The Appellant admits asking another person to handle his computer equipment to ship it to him in Senegal. He also admits using the SIM card from his employer-provided cell phone and his computer to work while in another country. I find that the Appellant acted as the employer says he did.

### Is the reason for the Appellant's dismissal misconduct under the law?

- [11] A worker who is let go because of misconduct can't get El benefits.
- [12] To be misconduct under the Act, the conduct has to be wilful. This means that the conduct is conscious, deliberate, or intentional.<sup>2</sup> Misconduct is conduct that is so reckless that it is almost wilful.<sup>3</sup> The Appellant doesn't need to have wrongful intent (in other words, he doesn't have to mean to be doing something wrong) for his behaviour to be misconduct under the law.<sup>4</sup>

<sup>&</sup>lt;sup>2</sup> See Mishibinijima v Canada (Attorney General), 2007 FCA 36.

<sup>&</sup>lt;sup>3</sup> See McKay-Eden v Her Majesty the Queen, A-402-96.

<sup>&</sup>lt;sup>4</sup> See Attorney General of Canada v Secours, A-352-94.

- [13] There is misconduct if the Appellant knew or should have known that his conduct could get in the way of carrying out his duties toward his employer and that there was a real possibility of being let go because of that.<sup>5</sup>
- [14] The Commission has to prove that the Appellant lost his job because of misconduct. The Commission has to prove this on a balance of probabilities. This means that it has to show that it is more likely than not that the Appellant lost his job because of misconduct.<sup>6</sup>
- [15] The Appellant says he was on vacation in Senegal until August 9, 2021. While on vacation, he got COVID-19. He says he was afraid of losing his job and decided to have his computer equipment shipped to Senegal to continue working until he could return to Canada.
- [16] The Commission argues that the Appellant knew the employer's rules and was aware that he could be let go if he didn't follow those security rules, since he got yearly training on security. The Commission says that the Appellant should have known that it was against the employer's policy to have his computer equipment shipped out of the country and to work outside Canada.
- [17] A manager working for the employer says that, to avoid putting customers' personal information at risk, computer equipment can't be shipped abroad without permission. This is because the company's rules say that employees should always have their computer equipment with them when out of office. This person argues that, if the Appellant could not return to Canada, he could have just explained the situation, and he would have been granted leave.
- [18] The Appellant told the Commission he was never made aware of the security rules for employees working remotely and says that he had no bad intentions behind his

<sup>&</sup>lt;sup>5</sup> See Mishibinijima v Canada (Attorney General), 2007 FCA 36.

<sup>&</sup>lt;sup>6</sup> See Minister of Employment and Immigration v Bartone, A-369-88.

actions. He says that the employer had to have known that he was working from Senegal since he told it that he would be vacationing in that country.

- [19] The Appellant's vacation ended on August 9, 2021. He emailed his supervisor to tell him he would be absent that day but got an automatic reply telling him that the supervisor was on vacation. Apparently, he then contacted the person filling in for his supervisor to tell this person that he would be absent for a day and that he would be working remotely after.
- [20] The Appellant says he already had permission to work remotely and that he had already told the employer the names of the people who were living with him and had access to his computer equipment. He says that one of those people prepared his equipment for shipping. The Appellant says that the only thing that was shipped to him was a computer case, since he got a monitor, keyboard, mouse, and other accessories in Senegal.
- [21] The Appellant also says that, to be able to log in remotely, he needed a code that was authorized by a supervisor. Since his supervisor was on vacation, someone else gave the Appellant this code.
- [22] The Appellant says that he contacted the Telus IT department for help logging in remotely. For this reason, he says that the employer knew he was logging in from another country.
- [23] The Appellant worked remotely from Senegal from August 10, 2021, to August 26, 2021. On August 26, 2021, the Appellant was told by the fraud department that he wasn't allowed to work from Senegal.
- [24] Since the Appellant hadn't told the employer that he was working from that country, the employer had to shut down some services to find out which employee was logged in outside Canada. The employer's head of human resources said that the Appellant's actions affected 250 employees, and nearly 5,000 Telus customers could not talk to a representative while services were shut down.

- [25] When he returned from his vacation, the supervisor told the Appellant that he wasn't allowed to work from Senegal and asked him to return to Canada as soon as possible. Then, the supervisor let the Appellant go for not following the company's security rules.
- [26] The employer argues that all employees, including the Appellant, get training on security rules when hired, and that all employees are trained yearly to get a refresher on security rules. It says that the Appellant handled confidential information.
- [27] The head of human resources submitted a document indicating the four conditions to be met for an employee to work remotely. They include a secure workspace and being within 150 kilometres of company premises.<sup>7</sup>
- [28] Although the Appellant argues that he didn't get any training on security rules, that no training was given on remote work, and that he was never told he could not work from another country, when he willingly agreed to work remotely, he accepted the four conditions. He should have had a secure workspace to avoid putting customers' confidential information at risk, and he could not work in a place that wasn't within 150 kilometres of company premises. The document explicitly says so.<sup>8</sup>
- [29] This document says that confidential information has to be protected and that security rules on remote work are accepted by the employee to prevent unauthorized access. For this reason, sharing the employer-provided computer isn't allowed.
- [30] I have to make this decision on a balance of probabilities. Although I understand that the Appellant didn't have any bad intentions and that he didn't mean any harm in doing what he did, he put the personal information of many customers at risk by not following the employer's policies. The Appellant didn't want to lose his job and acted without the employer's permission and without giving the employer key information about his situation. He got a code to work remotely but didn't tell the IT department or the person replacing his supervisor that he was still in Senegal. He didn't tell them that

\_

<sup>&</sup>lt;sup>7</sup> GD3-28.

<sup>&</sup>lt;sup>8</sup> GD3-28 to GD3-35.

he had asked someone to ship his computer equipment to Senegal and that he would work from that country.

- [31] By acting as he did, the Appellant broke the company's security rules.
- [32] Although he didn't want to lose his job, the Appellant could expect that he would be let go by not telling the employer that he was having his computer case or laptop shipped to a country that wasn't Canada and that he was working remotely from another country. Although the Appellant testified that he got an access code to work remotely that only a supervisor could give him, he didn't tell this person that he was working from Senegal.
- [33] The Appellant acted without the employer's permission and had his computer case shipped to him during his vacation for missing only one day of work. In Senegal, he got his computer equipment that had been shipped from Canada by someone else, and he was able to start working the day after his vacation ended. However, his computer case was handled by a third party and shipped, while the security rules say that employees who agree to work remotely should either always be with their computer equipment when out of office or make sure to leave it in a safe place. This is to avoid putting customers' confidential information at risk. Also, the Appellant wasn't allowed to work in a place that wasn't within 150 kilometres of Telus premises. If he was in doubt, he should have asked whether he could do so.
- [34] By not telling the employer such important information, the Appellant acted without permission and, in this situation, it seems he completely ignored the employer's rules to hide from it key details that went against the rules.
- [35] For this reason, I find that the Appellant could expect that he would be let go by acting this way.
- [36] Contrary to what he argues, the Appellant was told of the rules on remote work since he had to accept them to get permission to work remotely. Even though the Appellant said that the employer had to have known that he was working from Senegal

because he had told it he would be vacationing there, he deliberately didn't ask for permission to ship the computer equipment abroad, and he didn't clearly tell the employer that he intended to work from Senegal.

- [37] The Appellant's actions were reprehensible since he didn't follow the security rules, had the employer's computer equipment shipped to him, and used it in another country. This is against the employer's security rules and affected the employer. This is misconduct under the Act. The facts show that the Appellant didn't follow the employer's rules on the confidential information he handled and that he didn't clearly tell his employer about his situation.
- [38] This situation seriously affected the employer, who had to restrict computer access for over 250 employees. Also, nearly 4,500 calls from Telus customers could not be answered.
- [39] The supervisor let the Appellant go for gross negligence because he hadn't followed the company's rules. The employer didn't know that the Appellant was working from Senegal, since the fraud department had to investigate to determine who was working from that country.
- [40] I find that the employer's guidelines were clear to the Appellant and that he should not only have followed the security rules, but also respected customers' personal information.
- [41] The Appellant was let go for having computer equipment shipped to him in Senegal and for logging in from another country to work without permission. I find that this is misconduct.

## So, did the Appellant lose his job because of misconduct?

[42] In this case, I have to decide whether the Appellant acted as the employer says he did and whether that is misconduct under the Act.

[43] Based on my findings above, I find that the Appellant lost his job because of misconduct. The Appellant didn't get permission to ship employer-provided computer equipment to Senegal, and he didn't get permission to work from Senegal. The Appellant deliberately didn't tell the employer about his situation.

## Conclusion

[44] This means that the appeal is dismissed.

Josée Langlois

Member, General Division – Employment Insurance Section