ALERT MEMORANDUM

Defensive Controls: The Italian Supreme Court Outlines the Employer's Duties

November 13, 2023

In decision No. 18168 of June 26, 2023, the Labor Section of the Italian Supreme Court provides clarifications on so-called "defensive controls" ("*controlli difensivi*") carried out by employers.

From a substantive point of view, the Italian Supreme Court confirmed the distinction between "*controls necessary to protect corporate assets*", which are subject to Article 4 of Law No. 300 of 1970 (the "**Workers' Statute**") and defensive controls (which are not subject to that article) and set out the requirements of defensive controls.

From a procedural point of view, the Italian Supreme Court addresses the issues of the burden of proof and the admissibility of the findings arising from defensive controls.

The decision is an important development in the case law on defensive controls. In particular, while the decision imposes the burden of proving the lawfulness of the controls on the employer, it also provides employers with useful cues to assess when and how to resort to defensive controls and to prepare in advance to maximize the chances that courts will find the controls lawful when a disciplinary dismissal is challenged.

For questions regarding the issues discussed in this note, you may contact any of our firm's attorneys with whom you are in regular contact or the authors below.

ROME

Giuseppe Scassellati-Sforzolini
+39 06 6952 2220
gscassellati@cgsh.com

Andrea Mantovani
+39 06 6952 2804
amantovani@cgsh.com

Marco Accorroni
+39 06 6952 2320
maccorroni@cgsh.com

MILAN

Elena Galimberti
+39 02 7260 8670
egalimberti@cgsh.com

1. DEFENSIVE CONTROLS

The decision is an important development in the case law[1] allowing forms of monitoring that employers may carry out without having to abide by the requirements of Article 4 of the Workers' Statute, which aims to protect employees.

This provision was introduced: (i) to prohibit the use of monitoring tools for the purpose of covertly controlling employees' work activities; and, at the same time, (ii) to regulate the use of these tools when "*required by organizational and production needs or workplace safety*" since their use may incidentally lead to the control of employees' work activities (so-called unintentional controls). In particular, Article 4 provides that unintentional controls could only take place following a collective agreement or, failing that, upon authorization from the National Labor Inspectorate.

Over time, however, the need arose to exclude from the scope of Article 4 of the Workers' Statute controls carried out for the specific purpose of detecting unlawful conduct of employees, especially in case of conduct harming corporate assets or reputation. The need to negotiate with trade unions (which was potentially time-consuming and could also lead to no agreement) or to obtain authorizations (which implied the risk of imposing excessive restrictions and conditions) appeared to conflict with the employers' interest in detecting and taking action against employees' misconduct.

For this reason, the case law created the category of "defensive controls"[2] in order to exclude these forms of monitoring from the scope of Article 4 of the Workers' Statute and progressively defined the regulation of such controls by referring to the principles of good faith and fairness, as well as adequacy and proportionality as limits to the employers' conduct.[3]

Defensive controls may be carried out in different forms. For example, the Supreme Court has categorized as forms of defensive controls:

(a) checking corporate e-mails;[4]

(b) using video recordings;[5]

(c) checking internet connections;[6]

(d) controlling data traffic on company's pc;[7] and

(e) controlling employee attendance recorded by using company badges.[8]

It has been argued that the category of defensive controls was eliminated by the so-called *Jobs Act* in 2015,[9] which broadly extended the scope of Article 4 of the Workers' Statute to also include those controls carried out by the employer for the "*protection of corporate assets.*"[10]

However, the Supreme Court recently rejected this interpretation, finding a residual scope of the category of defensive controls by distinguishing between defensive controls "*in a broad sense*" and defensive controls "*in a narrow sense.*"[11]

According to the Supreme Court, defensive controls "*in a broad sense"* (or "*controls necessary to protect corporate assets*") concern all employees (or groups of employees) in the "*ordinary performance*" of their work, when they come into contact with corporate assets. Following the *Jobs Act* reform, these controls must be carried out in compliance with Article 4 of the Workers' Statute.

In contrast, defensive controls "*in a narrow sense*" are those aimed at ascertaining specific wrongful conducts attributable to individual employees. Such conduct falls outside the scope of Article 4 of the Workers' Statute,[12] since they do not concern the "*ordinary performance*" of employee's work. However, these controls are lawful only if there

[1] See, most recently, Supreme Court, Labor Section, July 20, 2023, No. 21681.
[2] See, Supreme Court, Labor Section, April 3, 2002, No. 4746.
[3] See, among others, Supreme Court, May 27, 2015, No. 10955; and Supreme Court, Labor Section, November 10, 2017, No. 26682.
[4] Most recently, see the decision under review.
[5] Supreme Court, Labor Section, November 8, 2016, No. 22662.
[6] Supreme Court, Labor Section, June 15, 2017, No. 14862.
[7] Supreme Court, Labor Section, September 22, 2021, No. 25732.
[8] Supreme Court, Labor Section, August 21, 2018, No. 20879.
[9] Law No. 183/2014.
[10] See Article 23 of Legislative Decree No. 151 of September 14, 2015 (implementing the enabling act of December 10, 2014, No. 183).
[11] Supreme Court, Labor Section, September 22, 2021, No. 25732 and Supreme Court, Labor Section, November 12, 2021, No. 34092; conversely Court of Milan, March 31, 2004, Court of Milan, April 11, 2005, and Court of. Rome, June 4, 2005.
[12] Supreme Court, Labor Section, September 22, 2021, No. 25732, para. 32.

is a "*grounded suspicion*" of wrongful conduct and they are proportionate to the employer's purpose.[13] The absence of any of these requirements results in the exclusion of the findings of the defensive controls as evidence in disciplinary proceedings against the employees.[14]

The decision refers to that case law and provides further clarification on the matter. In particular, the decision: (i) clarifies the notion of "*grounded suspicion*" which justifies the defensive controls; and (ii) outlines the criteria to balance employer's interests against employee's right to privacy.

The decision also: (i) clarifies that, in a lawsuit for wrongful dismissal, the employer bears the burden of proving the lawfulness of defensive controls; and (ii) states that failing to discharge this burden of proof results in the exclusion of the findings of the defensive controls as well as their products as evidence against the employee.

2. THE CASE

The case arises from a wrongful termination lawsuit. In particular, the employee complained that the evidence used by the employer as the basis for its disciplinary charges had been obtained through wrongful investigatory activities. The Court upheld employee's appeal, ruling that: (i) the inspection of their corporate e-mail was unlawful as it had been conducted without any justification; and (ii) the surveillance of the employee was unlawful because it was justified only based on the evidence contained in the inspected e-mails, which, as stated above, had been unlawfully obtained.

The monitoring of the employee's e-mail box was considered not proportionate to the purpose pursued by the employer, since it indiscriminately concerned all communications stored on employee's work computer and the employer did not demonstrate that it had informed the employee in advance of the possibility of such monitoring.

The Supreme Court, in rejecting the employer's appeal, found that the lower court had correctly ruled in accordance with the principles governing the matter.

3. LAWFULNESS REQUIREMENTS

According to the Supreme Court defensive controls can be carried out only where: (i) they are based on justifiable grounds; and (ii) they are conducted in a manner that respects employee's right to privacy.

This is because, the category of defensive controls raises the risk of wrongful monitoring of work performance and, in the absence of the guarantees set out in Article 4 of the Workers' Statute, could also justify monitoring that is otherwise harmful to employees' dignity and privacy.

3.1. EXISTENCE OF JUSTIFIABLE REQUIREMENTS: "GROUNDED SUSPICION"

The Supreme Court clarifies that the employer may only conduct defensive controls when there is "*actual indicative evidence*" that gives rise to a "*grounded suspicion*"[15] of unlawful conduct (pp. 7 and 9).[16] Therefore, employer's "*purely personal belief*" is not sufficient, as "*objective confirmation of the legitimacy of the purpose of the defensive control*" is required (p. 9). This means that, in accordance with the European Court of Human Rights ("ECtHR") case law on employee controls, indicative evidence must be "*material and identifiable*", so much that they would lead a reasonable person to suspect that the employee to be monitored has engaged in misconduct (p. 11).[17]

In addition, a lack of evidence at the time of monitoring may not be remedied by evidence obtained later.

[13] *Ibid.* para. 35.

[14] See, among others, Supreme Court, Labor Section, October 5, 2016, No. 19922; and Supreme Court, Labor Section, October 1, 2012, No. 16622.

[15] Regarding the search for evidence in support of the grounded suspicion, please note that recently the ISO/TC 309 Technical Committee published Guidelines ISO/TS 37008:2023, July 2023 (Internal investigations of organizations – Guidance); in particular, please refer to paragraph 8.8 (Evidence) of that Guideline.

[16] In contrast, Supreme Court, Labor Section, May 2, 2017, No. 10636, according to which the mere assumption that wrongdoing is in progress is sufficient.

[17] European Court of Human Rights, Grand Chamber, *Lopez Ribalda et al.v. Spain*, October 17, 2019.

3.2. PROPORTIONALITY OF CONTROL AND COMPLIANCE WITH OTHER DATA PROTECTION PRINCIPLES

The Supreme Court also points out that defensive controls must be carried out in compliance with the employee's privacy rights under Article 8 of the European Convention on Human Rights (the "ECHR").

Accordingly, before deciding whether to carry out defensive controls and determining their form, scope and duration, it is necessary to balance the employer's interests that may be jeopardized by the employee's conduct against the employee's privacy and dignity. The prior assessment required from the employer must also be aimed at verifying the compliance with the principles of proportionality, minimization, non-excessiveness in relation to a legitimate purpose, transparency and fairness as set out in the General Data Protection Regulation (EU Regulation No. 2016/679; the "GDPR").

The positive outcome of the mentioned balancing test, showing that the employer's interest outweighs the conflicting interests or fundamental rights and freedoms of the data subjects, may allow the employer to rely on its legitimate interest under Article 6(1)(f) of the GDPR[18] as the legal basis for processing employees' personal data in the context of the investigation.

The lawfulness of defensive controls may instead be challenged where, considering "*the totality of the circumstances*" (p. 15), the mentioned principles are infringed. As guidance for the merits courts, the Supreme Court recalled the criteria that the ECtHR has identified for the purpose of assessing compliance of employer's surveillance measures with Article 8 ECHR. In particular, the merits courts will have to assess:

i. whether the employee was informed in advance and clearly about the possibility for the employer to carry out defensive controls;

ii. whether the controls are excessively invasive of employee's privacy, taking into account their nature, the place where they take place, their duration, and the number of people who have access to their results;

iii. whether the employer provides sufficiently serious reasons to justify the specific control measure adopted;

iv. whether employer's purpose could have been achieved in another, less intrusive manner;

v. whether the employer used the information obtained from the control only to achieve the declared purpose; and

vi. whether the employer has provided the employee with adequate safeguards on the degree of intrusiveness of the control measures by means of prior information to the employees concerned, their representatives or an independent body, or by the provision of grievance mechanisms.[19]

Furthermore, data protection legislation itself obliges the employer to inform its employees under Article 13 GDPR about the possibility of conducting such controls, in accordance with the principle of transparency under Article 5(1)(a) GDPR.

4. BURDEN OF PROOF

According to the Supreme Court, the burden of alleging and proving the factual elements that constitute the "*grounded suspicion*" authorizing defensive controls in the context of a wrongful termination case falls on the employer, given that, in accordance with the principle of proximity of evidence, the latter has a greater opportunity to know those factual elements, either directly or indirectly.

In addition, the employer has the burden of proving the circumstances justifying the controls carried out in the absence of the general guarantees provided for in Article 4 of the Workers' Statute also because, more generally, it is on the employer to prove all the elements justifying the dismissal of the employee, in accordance with Article 5 of Law No. 604/1966.

The decision does not explicitly clarify which

[18] Article 6(1)(f) of the GDPR allows the processing of personal data if "*necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.*"

[19] European Court of Human Rights, Grand Chamber, *Bărbulescu v. Romania,* September 5, 2017.

party bears the burden of proving employer's compliance with the principles of proportionality and privacy rights. However, the Supreme Court appears to burden the employer of the proof of those facts as well.[20] Indeed, the Court considered the lack of evidence concerning certain circumstances (including prior information about the controls) in order to uphold the decision on the merits overturning the dismissal, including its finding that the defensive controls were carried out in violation of data protection principles.

5. CONSEQUENCES OF FAILURE TO COMPLY WITH THE LAWFULNESS REQUIREMENTS

The Supreme Court judgment also clarifies that the procedural penalty for infringing the lawfulness requirements for defensive controls is the same as that applied by the case law in case of unlawful controls necessary to protect corporate assets, *i.e.*, the exclusion of any evidence resulting from the controls in the context of disciplinary proceedings against the employees (p. 13).[21] It follows that, based on a mechanism that can be traced back to the so-called "*fruit of the poisonous tree*" doctrine, evidence drawn from unlawful defensive controls cannot be used to prove the existence of a "*grounded suspicion*" that would justify further controls carried out by the employer.[22]

6. CONCLUSIONS

The decision provides important guidance for employers intending to protect themselves against their employees' disciplinary misconduct.

In particular, the Supreme Court confirmed that, in the absence of the guarantees under Article 4 of the Workers' Statute, the employer is still subject to strict obligations. Compliance with these obligations must then be demonstrated in court if the employee challenges his dismissal as based on evidence gathered through unlawful defensive controls.

In light of the above, defensive controls should be carried out only after a careful assessment, based on all available information, of the requirements set out by this decision, especially the "*grounded suspicion*" of misconduct.

If, as a result of this assessment, there is actual indicative evidence supporting the suspicion of misconduct, the employer should then consider whether the misconduct could be ascertained by means of controls that are compliant with Article 4 of the Workers' Statute. If it could not be ascertained by such controls, the employer should choose the control measures and implementation methods that would enable the detection of the misconduct with the least invasion of the employee's privacy, taking into account the circumstances in which the control is carried out and the seriousness of the misconduct.

In addition, given the importance recognized by the Supreme Court to prior information provided to the employee, the employer should provide documents that allow employees to know the possible forms of control and the safeguards in place for their protection.

For instance, in the case at issue, controls were carried out on corporate devices entrusted to the employee (such as laptops and smartphones).

In order to conduct defensive control the employer should also (i) implement a policy governing the use of the tools provided to employees and (ii) mention in the notice provided to employees

[20] See Court of Appeal Rome, January 19, 2022, No. 67.

[21] See above, note 14.

[22] In holding the exclusion of evidence in breach of privacy regulations, the decision applies Article 11, paragraph 2, of Legislative Decree No. 196 of 2003 (the "Privacy Code"), "*in the wording in force at the time of the facts*", according to which "[p]*ersonal data processed in violation of the relevant data protection legislation may not be used.*" However, following the reform of the Privacy Code pursuant to Legislative Decree No. 101 of August 10, 2018, the matter is now regulated by Article 2-*decies* of the Privacy Code. Despite confirming that personal data processed in violation of the relevant regulations may not be admitted in evidence, this provision also states that Article 160-*bis* of the Privacy Code still must apply. According to Article 160-*bis*, "[t]*he validity, effectiveness and admissibility in judicial proceedings of deeds, documents and measures based on the processing of personal data that do not comply with provisions of the law or regulations shall remain governed by the relevant procedural provisions.*"
Given that the Civil Procedure Code does not provide for exclusion of evidence obtained in breach of a legal provision, it appears that, under the procedural rules currently in force, evidence that would be inadmissible outside civil proceedings may still be admitted in a subsequent civil proceeding. However, the issue remains open. Indeed, while some local courts state that "*the violation of the rule of conduct does not result in the exclusion of the data*" (Court of Perugia, Labor Section, April 13, 2021, No. 112), the Labor Section of the Supreme Court has not yet clarified its stance on the matter (see, most recently, Supreme Court, Labor Section, October 11, 2023, No. 28378, in which, while raising the issue, the Court held that there was no need to "*examine* [it] *thoroughly* [...] *since the scope of the reform of 2018* [did] *not apply* ratione temporis *to the case at issue*").

under the GDPR that such controls may be carried out if there is a grounded suspicion of disciplinary misconduct.

…

CLEARY GOTTLIEB