Law Shopping in Relation to Data Processing in the Context of Employment: The Dark Side of the EU System for Criminal Judicial Cooperation?

This post was written by Ms Martina Mantovani, Research Fellow at the Max Planck Institute Luxembourg. The author is grateful to her colleague, Ms Adriani Dori, for pointing out the tweet.

On 26th September 2019, Dutch MEP Sophie in 't Veld announced through her Twitter account the lodging of a question for written answer to the EU Commission, prompting the opening of an investigation (and, eventually, of infringement proceedings) in relation to a commercial use of the European Criminal Record Information System (ECRIS). A cornerstone of judicial cooperation in criminal matters, this network is allegedly being exploited by a commercial company operating on the European market (hereinafter name, for the purposes of this entry, The Company), in order to provide, against payment, a speedy and efficient service to actual or prospective employers, wishing to access the criminal records of current employees or prospect hires.

Commercial activities of this kind raise a number of questions concerning, first and foremost, the lawfulness of the use of the ECRIS network beyond its institutional purpose, as well as the potential liability under EU law of the national authorities which are (more or less knowingly) fostering such practices. Moreover, as specifically concerns the topic of interest of this blog, such commercial practices exemplify how law shopping, stemming from the lack of coordination of Member States' data protection laws, can be turned into a veritable profit-seeking commercial endeavor. As it is, these commercial practices are made possible not only by the specific legislation instituting the ECRIS, but also due to the legal uncertainty and fragmentation fostered by the GDPR. In fact, this Regulation leaves rooms for maneuver for Member States' legislators to specify its provisions in relation to, *inter alia*, the processing of personal data in

the context of employment (art 88), without nonetheless providing for either a guiding criterion or an explicit uniform rule to delimit or coordinate the geographical scope of application of national provisions enacted on this basis. This contributes to creating a situation whereby advantage might be taken of the uncertainty relating to the applicable data protection regime, to the detriment of the fundamental right to data protection of actual or prospective employees.

The ECRIS: institutional mission and open concerns.

The ECRIS is based on two separate but related pieces of legislation, Council Framework Decision 2009/315/JHA and Council Decision 2009/316/JHA, as well as on a separate data protection framework, previously set out by Council Framework Decision 2008/977/JHA, now repealed and replaced by Directive (EU) 2016/680. The intuitional mission of the ECRIS consists in providing competent public authorities from one Member States with access to information from the criminal records of nationals of other Member States. By facilitating the exchange of information from criminal records, this network aims at informing the authorities responsible for the criminal justice system of the background of a person subject to legal proceedings, so that his/her previous convictions can be taken into account to adapt the decision to the individual situation (Recital 15 of Council Framework Decision 2009/315/JHA). The ECRIS additionally aims at ensuring that a person convicted of a sexual offence against children will no longer be able to conceal this conviction or disqualification with a view to performing professional activity related to supervision of children in another Member State (Recital 12 of Council Framework Decision 2009/315/JHA, in conjunction with article 10(3) of Directive 2011/93/EU). In current law, ECRIS applications for accessing extracts from criminal records can be filed by judicial or competent administrative authorities, such as bodies authorized to vet persons for sensitive employment or firearms ownership. In such cases, these applications must be submitted with the central authority of the Member State to which the applicant authority belongs. This central authority may (and not *shall*) submit the request to the central authority of another Member State in accordance with its national law. In addition, access requests can also be filed by the person concerned for information on own criminal records. In this case, the central authority of the Member State in which the request is made may, in accordance with its national law, submit a request to the central authority of another Member State for information and related data to be extracted from its criminal record,

provided the person concerned is or was a resident or a national of either the requesting or the requested Member State. In relation to information extracted via the ECRIS for any purposes other than that of criminal proceedings, a Statewatch Report of 2011 already expressed serious concerns, noting that while the European Data Protection Supervisor recommended that requests of this kind should have only be allowed "under exceptional circumstances", the Council Framework Decision did not finally introduce such a stringent limitation. Moreover, since, under current article 7, the requested central authority shall reply to such requests *in accordance with its national law*, this piece of legislation provides "*an opportunity for the widespread cross-border exchange of information extracted from criminal records for a variety of purposes unrelated to criminal proceedings*". That same Report additionally stresses the huge potential for "information shopping" that may thus arise, insofar as applicants who are not able to obtain information on an individual from that person's home Member State, may access it via another Member State which also holds the information and has less stringent data protection legislation.

New commercial practices.

It is within this framework that the new commercial practices lying at the heart of Ms Sophie in 't Veld's question must be understood. The commercial services in question are provided by The Company, expressly identified in the MEP's interrogation. On its website, The Company takes great care to specify that, while it may have a name which closely echoes the EU system, it remains a private company offering commercial services and that "*the purpose of this similarity is to highlight [it uses] the EU structures to access information on criminal records*". According to the same source, the services provided aim at addressing a widespread need of employers from Europe and rest of the world, who wish to ensure that their employees have no criminal background. Having remarked that said employers often struggle to perform background checks in a compliant manner, with legislation varying across the European Union rendering such a check "*complicated, time consuming or impossible*", The Company proposes an innovative solution. According to its website, it "discovered" that by resorting to a EU program called European Criminal Records Information System, it is "*able to address all of those concerns and offer easy and compliant access to state-issued EU criminal records certificates*". The FAQs further specify how this procedure works in practice. They confirm that all certificates are obtained from central

criminal registers of EU Member States. What makes the service provided "unique" is that The Company is declaredly streamlining all access requests through the ECRIS central authority of just one Member State, who requests criminal information from its European counterparts on The Company's behalf. According to both The Company's website and MEP Sophie in 't Veld's interrogation, the National Criminal Register of this Country "*play[s] a role of a middleman in the flow of documentation and requests the information from the central register of the destined country*". While The Company claims that "*the application is made with the applicant's full awareness and explicit consent*", the MEP stresses "*it is not clear whether the person whose records are obtained has given explicit consent*". In fact, it must be acknowledged that the website's wording is rather ambiguous, being unclear whether the expression "*the applicant*" refers to the employer seeking the company's services, or to the persons whose criminal records are being accessed. The way in which The Company (which, incidentally, has UK phone number and which, according its website's FAQ's, seems to direct its services primarily to employers operating in the UK and Ireland) is effectively resorting to a foreign National Criminal Register for accessing the ECRIS remains a mystery. In fact, The Company cannot certainly be counted among either the administrative or the judicial authorities admitted to filing a request under Council Framework Decision 2009/315/JHA. Two highly speculative guesses might be made. A first possibility might be that the National Criminal Register allegedly playing the role of middleman might be misapplying the Framework Decision by submitting requests filed by non-legitimate applicants (as MEP in 't Veld seems to imply, by appealing to the principle of mutual trust and by envisioning the possibility of opening infringement proceedings). As it is, the form for access requests used by said National Criminal Register does not strictly require, according to its letter, that person filing the request shall be the same person whose criminal records need to be obtained, although it contains the explicit warning that "obtaining unauthorized information about a person from the National Criminal Register is punishable by a fine, restriction of liberty or imprisonment up to 2 years". A second possibility is that the company might be exploiting individual access requests, which – it must be stressed – could concern only "residents or nationals *of the requesting or requested Member State*" (article 6§2 of Council Framework Decision 2009/315/JHA). In such cases, one might imagine that, after being approached by the employer, The Company would transmit the aforementioned form to the employee/prospect hire, who would personally sign the form, thus

explicitly consenting to the procedure. From the standpoint of data protection law, however, such an approach would not be less problematic. As repeatedly confirmed by the Article 29 Working Party, an employer which processes personal data (even within the framework of a recruitment process) qualifies as a controller of the employee/prospect hire personal data, having moreover very limited possibilities to rely on the employee's express consent as a lawful basis for their processing. Furthermore, such approach remains even more controversial if account is taken of the fact that it may be purposefully used to circumvent the more restrictive data protection provisions in matters of employment enacted by another Member State.

The Member State's law applicable to the processing of personal data in the context of employment.

Albeit having been promoted by the EU Commission as "a single, pan-European law for data protection", the new GDPR fails to level out all legislative differences in the Member States' data protection laws. As mentioned above, it provides in fact a margin of maneuver for Member States to specify its rules, including for the processing of special categories of personal data. To that extent, it does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful (recital 10). In this vein, its article 88 provides that "Member States *may*, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of recruitment […]". Commercial practices such as those signaled by Ms in 't Veld seem to thrive on this situation of persisting legal uncertainty and fragmentation. In fact, some Member States' data protection legislation expressly prohibits the use of individual access requests to criminal record in connection with the recruitment of an employee, except for very exceptional circumstances. Nonetheless, such legislative measures are often rendered toothless at the international level, either because the legislator limited – more or less willingly – their reach to the domestic domain, or because their geographical scope of application, left undefined by the relevant GDPR-complementing law, remains highly ambiguous. This is precisely what happens in relation to the British and the Irish Data Protection Acts, expressly mentioned by The Company's website.

- *The UK Data Protection Act 2018*

This law, meant to adapt the UK data protection regime to the GDPR, provides, under its *Section 184,* that:

"it is an offence for a person ("P1") to require another person to provide P1 with, or give P1 access to, a relevant record in connection with— (a)the recruitment of an employee by P1; (b)the continued employment of a person by P1; or (c)a contract for the provision of services to P1." According to *Schedule 18* of the same law, *"relevant record" means—* […] *(b)a relevant record relating to a conviction or caution …*[which] *(a)has been or is to be obtained by a data subject in the exercise of a data subject access right from a person listed in sub-paragraph (2), and (b)contains information relating to a conviction or caution.* The Company is well aware of these restrictions, which are expressly reported on its website (reference is made to Section 56 of the Data Protection Act (DPA) 2015, corresponding to Section 184 of the new DPA 2018). Nonetheless, it is further clarified that "[*The Company] do[es] not make any requests under section [184] of the DPA, therefore [being] not limited by [it]*" and that, consequently, it might even be "*safer*", as a UK-based employer, to resort to its services. And this might admittedly be true, since the prohibition set out by Section 184 solely concerns records obtained by a data subject in the exercise his/her access right from one of the UK-based authorities listed in §3(2) of Schedule 18, and not by a foreign Criminal Register. Nonetheless, despite the apparent lawfulness of the whole process, the fact remains that the use (or abuse?) of an EU system, established to address specific needs of the judicial cooperation in criminal matters, becomes, in practice, the tool for enabling a UK-established employer to access employees' personal data which he could not lawfully access domestically. This goes explicitly against the declared ratio and aim of Section 184 of the UK Data Protection Act. As clarified by the Explanatory Notes, this provision aims at thwarting conducts which may give the employer access to records which they would not otherwise have been entitled. There are, in fact, established legal routes for employers and public service providers to carry out background checks, which do not rely on them obtaining information via subject access requests. Disclosure and Barring Service (DBS) checks can in fact be performed *locally* only by one responsible organizations registered with DBS and according to the procedure and guarantees set out by British law.

- *The Irish Data Protection Act 2018*

The other relevant national GDPR-complementing provision is Section 4 of this law, entitled "obligation not to require data subject to exercise right of access under Data Protection Regulation and Directive in certain circumstances". This provision prohibits a person from requiring, in connection with the recruitment of an individual as an employee or his continued employment, that individual to exercise his rights of access to own criminal records, or to supply the employer with data obtained as a result of such a request. Again, The Company's website specifies that the services provided are not based on requests under Section 4 of the Irish law, and that this provision does not consequently constitute a limitation, thus making the use of their services "safer" for employers. It must be noted, however, that as opposed to the British provision, Section 4 does not limit the scope of the prohibition to records obtained by requesting access to Irish authorities. Therefore, the extent to which the processing of employees' personal data, including their criminal records, will be covered by Section 4 of the Irish Data Protection Act will finally depend on the identification of the scope of application of this Act *as a whole*. The problem with the Irish Data Protection Act (and with many other national GDPR-complementing laws, such as, *inter alia,* the Italian and the Spanish legislations) is that it does not explicitly define its geographical reach, thus fostering uncertainty as to the range of factual situations effectively covered and governed by its complementing provisions. This omission has been maintained in the final text of the Irish Data Protection Act despite the contrary advice given, during the drafting process, by the Irish Law Society. This pointed to such a lacuna as a potential source of ambiguity, for both individuals and controllers/processors, with regard to the remit and applicability of that piece of legislation. In particular, clarity as to what entities the Data Protection Act 2018 applies would have been especially desirous "given the number of corporations processing personal data on a large scale in Ireland and the likely queries that might otherwise arise and require judicial clarification".

The need for better coordination of national data protection laws in the context of employment.

Following Ms in 't Veld's question, the EU Commission will eventually investigate whether such a use of the ECRIS system is compliant with EU law, and whether the National Criminal Register in question is lawfully taking action on the basis of applications filed by/or with the help of The Company. In any event, the objective difficulties that may be encountered, in current law, in deciding over the

lawfulness of commercial practices this kind, which might be merely taking advantage of pre-existing legislative loopholes and gaps, are a clear cry for better coordination of the Member States' data protection laws enacted on the basis of the opening clauses enshrined in the GDPR. In a related paper, which is forthcoming in the *Rivista italiana di diritto internazionale privato e processuale,* this author tries and demonstrate that this problem is of an overarching nature, not being limited to the rather specific issues of, on the one side, the parochial approach adopted by the UK Parliament in defining the reach of its provision on forced access to criminal records for employment purposes and, on the other side, the silence kept by many national legislators concerning the geographical reach of their domestic data protection law. As it is, the entire European regime on data protection is deeply and adversely affected by a generalized lack of coordination of the spatial reach of domestic GDPR-complementing provisions. Lacking any uniform solution at EU level (set out either by the GDPR itself or by other existing instruments) the delimitation of the scope of application of national GDPR-complementing provisions is in fact left to unilateral and uncoordinated initiatives of domestic legislators. The review of existing national legislation evidences the variety of techniques and connecting factors employed for these purposes by the several Member States, which is liable to generate endemic risks of over- and under-regulations, and, above all, gaps of legal protection which are perfectly exemplified by, but not limited to, the commercial practices arisen in relation to the use of the ECRIS.