

Ireland's DNA Database Protecting Human Rights

ACJRD Conference 11 December 2020

Our session

- Legal basis for the DNA Database System
- Numbers & Matches
- Sampling & Destruction
- Key Human Rights Laws and Standards
- DNA Database System Oversight Committee
- Wrap up

Legal basis: 2014 Act

Parts 1 - 6 Taking of Samples

Part 8 DNA Database System

Part 9 DNA Database System Oversight Committee

Part 10 Destruction

Part 12 International Cooperation

Database operations from November 2015

Numbers & Matches

The number of profiles **38,747** (Dec 2019).

#1 Potential match – crime stain can match another crime stain, suggesting a link between crimes

#2 Potential match - crime stain can match to a person suggesting a link between the person and the crime.

780 hits in 2019 which assisted in **1,011** cases.

43%

43 out of every 100 crime scene samples uploaded onto the database will be linked to a person

Human Rights

Sources of Law and Standards

Constitution/Bunreacht na hEireann

European Convention on Human Rights (ECHR) Article 8

EU Charter of Fundamental Rights (Articles 7 and 8)

International Covenant on Civil and Political Rights (ICCPR) (Article 17)

Special Procedures. UN Special Rapporteur on the right to privacy

Human Rights

Key rights engaged in a DNA
Database System

Right to privacy

Right to bodily integrity

Right to protection of personal data

Non-discrimination/equal treatment

Right to a fair trial

Rights of crime victims

ECHR Standards

S. and Marper v. the United Kingdom (2008) ECHR 1581

- **Indefinite retention** in a database of the applicants' fingerprints, cell samples and DNA profiles after criminal proceedings against them had been terminated by an acquittal in one case and discontinued in the other case.
- Use of modern scientific techniques in the criminal-justice system could not be allowed at any cost and without carefully **balancing the potential benefits of the extensive use of such techniques against important private-life interests.**

Marper Standards

- Retention at issue had constituted a **disproportionate interference** with the applicants' right to respect for private life and could not be regarded as necessary in a democratic society.
- State bore responsibility for "**striking the right balance**".
- Conclusion: the **blanket and indiscriminate nature of the powers** of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in this particular case, failed to strike a fair balance between the competing public and private interests.

Key Human Rights Safeguards

- Legal basis for the collection and storage of samples
- Movement of data between collection point (AGS) and the database (FSI)
- Destruction – time limits
- Security of the systems
- Technical standards and quality assurance
- Independent oversight
- Safeguards in law
- Ethnic and minority overrepresentation on the database

DNA Database System Oversight Committee

Expertise

Legal, human rights, data protection, law enforcement, forensic science

In order to oversee:

Management and operation of the DDS for the purpose of maintaining the integrity and security of the system

Functions (ss. 71-74)

Receipt handling, transmission and storage

Generation of profiles - quality control and assurance

Accessibility, disclosure, security

Removal

AGS, GSOC, coroner

What we do

Meet 6 times a year

Work-plan each item under our functions

Examine detailed statistical information from FSI: samples added and removed, profiles matched and cases aided, live match data sharing under Prum

Discuss Prum operations, security and quality assurance

Interact closely with NFCO, other AGS members, criminal justice agencies

Produce an Annual Report (laid before the Houses)

Focusing on...

Personal data rights

Victims rights

Due process/fair procedures

Audits

System organisation

System culture

Effective resourcing

Key Challenges

See Annual Report 2019

1. Forensic Laboratory
 2. Security
 3. Garda staffing
 4. Non-submitted samples
-

Prum

EU Council Decisions
2008/615/JHA and
2008/616/JHA

Sharing DNA data with

- Austria since the 2nd October 2019
 - The Netherlands since the 7th February 2020
 - The United Kingdom since the 19th March 2020
 - Latvia since the 19th Aug 2020
-

Wrap up

Key tool in effective law enforcement and criminal justice system

Advancing the fulfillment of victims' rights

New system and problems have emerged

Very high value attaching to personal data, little room for error if any

Watch in the future:

- Changes to legal basis
- Numbers on the database
- Match accuracy leading to conviction

Thank you