Implementing the Protocol to the Convention on Cybercrime on Xenophobia and Racism: Good practice study

Alexander Brown

University of East Anglia (UEA)

The First Additional Protocol (pp. 27-30)

- Art. 3 creates a states party obligation to establish criminal offences of intentionally and without right distributing, or otherwise making available to the public, **racist and xenophobic material**, through a computer system
- Art. 4 creates a states party obligation to establish criminal offences of intentionally and without right **threatening** (with the commission of a criminal act) persons or a group of persons, through a computer system, based on race, colour, national or ethnic origin, religion
- Art. 5 creates a states party obligation to establish criminal offences of intentionally and publicly and without right **insulting** persons or a group of persons, through a computer system, , based on race, colour, national or ethnic origin, religion
- Art. 6 creates a states party obligation to establish criminal offences of distributing or otherwise making available to the public and without right, through a computer system, material which **denies, grossly minimises, approves or justifies acts constituting genocide or other atrocity crimes** as defined by international law

Methodology (pp. 13-15)

- The author(s) of the study used mixed methods to identify and uncover specific examples of good practice:
- Questionnaire on good practices completed by: France, Germany, Norway, Slovakia, and Spain
- Additional inputs from Brazil and Serbia
- Meta-survey of existing ECRI country reports
- Key term searches within the HUDOC database of case law of the European Court of Human Rights (ECtHR)
- Surveyed academic literature on hate speech and hate crime laws

Some standout good practices (p. 55):

- Courts: compatibility with the Protocol through interpretation
- Enforcement of existing laws
- Dedicated reporting mechanisms (e.g. online platforms, telephone hotlines)
- Systems for the collection, management and transparency of statistics on instances of unlawful hate speech and hate crime offences that occur on the Internet

Conti.

- Specialised authorities (e.g. special police cybercrime units, special public prosecutors for cybercrime)
- Co-operation, domestic and international levels, among different agencies and organisations (e.g. production orders, sharing information on suspects, case referrals, administrative and/or judicial notifications, judicial co-operation across state borders, coordinated enforcement actions, codes of ethics)
- Capacity-building in law enforcement (e.g. hiring more specialists, increased training, capacity management)

More creative and ambitious practices (p. 56):

- Special regulatory frameworks for social media platforms
- Supplementing the primary scheme of criminalisation targeting individual perpetrators with a secondary scheme of criminalisation aimed at the conduct of senior managers of social media platforms
- Amend constitution to directly and explicitly recognise limits to the right to freedom of expression with respect to ‘hate speech’ (i.e. using that specific term)
- Special guidance and awareness-raising campaigns for politicians, senior government officials, and heads of law enforcement authorities
- Harmonisation of legal standards for what counts as unlawful hate speech or hate crime offences committed on the Internet