Number	LANCS-D4.1-RN-D.1	A-PI--

Title	Research Note (RN) for D4.1
Subtitle	Ethical aspects of development **D** : *ICT for Human Security*

PROBLEM		SOLUTION	

Research Note	X		Selected Annotation	

Categories: | | |

Summary:

This note addresses the implementation and governance of ICTs for human security. It takes issue with the lack of purpose and direction as well as the lack of humility in decision-making on deploying advanced surveillance technologies and mobility controls.

CONTEXT

According to industry pundits, advanced ICTs are crucial to improve security. Accordingly, the official argument has been that public, private and corporate agencies need the new technologies to support, oversee and protect Western transnational market democracy and 'our way of life'. Systematic checks are made across agencies to monitor the activities of organizations, markets and trade, to profile and stereotype using data mining and statistical categorizations of 'dangerous' groups, to perform identity checks on citizens and foreigners, and to screen for behaviours in crowds and mundane activities. The latest advancements are transforming these practices with advanced sensory systems, mobile readers, sophisticated information processing and complex inspection and detection techniques, including ICT-assisted predictions of future events, all of which have implications for the relationship between individual rights and the public good (on profiling see Hildebrandt and Gutwirth, 2008; Hildebrandt, 2008). In other words, ever more sophisticated surveillance is the key ingredient in the recent securitization trend, with a gradual shift in emphasis and approach towards the surveillance of everything, essentially treating all persons, vehicles, transactions and cargo as suspect

(Key readings include Amoore, 2006; Balzacq and Carrera, 2006; Bigo and Guild, 2005; Bigo et al, 2007; Carrera, 2005; Council of the European Communities, 2000; Council of the European Union, 2009; Daskala and Maghiros, 2007; Daskala and Maghiros, 2007; De Hert, 2008; Edwards and Gill, 2003; Lodge, 2007b; Lyon, 2003; Raab and Bennettt, 1994).

FACTS

Decisions on the uses of ICTs for human security reflect on ethical questions of purpose or mission, how to adequately protect data on persons and property, and ensure fairness in the treatment of suspects and all other persons. Security has been the trope for promoting or opposing problems of immigration and border control, but very little has been done to engage wider publics, including a range of occupations who could be seen as legitimate stakeholders in debate and decision-making. Perhaps the biggest challenge for decision-makers is the limit of prediction in forecasting, i.e., ensuring that we actually have a realistic 'roadmap' to safer and more secure societies.

The tendency is to isolate or gloss over the scientific and technical expertise. Not only is it problematic for publics to be critically engaged, but also for ethicists, lawyers, politicians and regulators who all have designated roles in institutionalized decision-making processes. They are often unclear on what they are looking at from a technically operational perspective—what the potentials and limitations actually are—if the proposed systems will be robust, useful, usable and reliable for the purposes at hand. The involvement and economic gains of ICT-related industries also give rise to a number of suspicions. The new technologies are promoted in the name of a 'need for security' which often is loosely defined and rhetorically elevated. Solutions to problems of reliability and dependability do not seem to have the highest priority when industry spokespersons continue to promote more interoperability, more automated checking and less human intervention (see Lodge, 2007a on this issue).

COMMENT

In order to cultivate wider participation and more humility in assessment and decision-making on ICTs for human security, the assumptions on which 'security' already rests will have to give way to questions of purpose and direction (see Jasanoff, 2003 on a similar issue). It is also imperative to understand what means are necessary to intercept and influence the uses ICTs in early stages of development and deployment. As Wynne has pointed out (e.g., Wynne, 1992; Wynne, 1988), the framing of what the problems might be and which issues should be debated is typically confined to the imaginations of scientific, technological, policy and institutional expertise.

Developments that need constant reflection and debate involve:

- activities that require the crossing of actual and virtual borders or checkpoints
- activities that include being in non-spaces / transits, i.e., traffic hubs and infrastructures for:
    - cars
    - trains
    - trams
    - buses
    - aeroplanes
    - ships

Furthermore, the developments that complicate ethical reflection on questions of surveillance and security, are the private uses of ICTs (internet and mobile technologies) and the occupational uses of ICTs that operate and service such industries, including:

- shopping
- gaming
- social networking

A host of ethical issues are implicated for reflection and debate:

The border between physical and virtual reality
Automation in capturing / processing data on persons
Automation for security
Automation for tracking
Dignity and privacy
Data protection
Misuse and mishandling of data
Safety and liability
Identity theft
Fraud
Technological 'fix'