naprave – pa je mogoča vsaj delna zaščita pred tovrstnim prisluškovanjem. Strojne rešitve so oklepljanje kablov, elektronskih naprav ali celo celih stavb s kovino, kar prepreči »uhajanje« elektromagnetnih signalov, vendar pa so razmeroma drage. Za pametne kartice Kocher in sodelavci iz podjetja Cryptography Research predlagajo več rešitev, ki pa ravno tako zahtevajo posege v samo zasnovo pametnih kartic. Te rešitve niso poceni, pa tudi hitro dosegljive ne.

Za preprečevanje tempest napada na računalniški zaslon opisujeta Kuhn in Anderson neprimerno cenejšo programsko rešitev, in sicer uporabo posebnih tempest pisav (ang. *tempest prevention font*), s katerimi preprečimo, da bi prisluškovalcu uspelo rekonstruirati dovolj jasno sliko z nadzorovanega zaslona. Signal torej lahko prestreže, vendar si z njim ne more veliko pomagati. Poleg tega sta odkrila še dve metodi, s katerima bi bilo mogoče preprečiti prestrezanje signalov s tipkovnice in trdega diska, metodi pa bi bilo mogoče implementirati z manjšimi stroški z nadgraditvijo gonilnikov (Kuhn in Anderson 1998, 139). Za običajne uporabnike je danes na voljo le zaščita proti tempest napadu s tempest pisavami; vgrajena je v programski paket PGP.

Kriptografija in gibanje za elektronsko zasebnost

Če je v ozadju zahtev po čedalje večjem nadzoru potreba po maksimalno varni in predvidljivi družbi, pa se je s pojavom kriptografije pojavil strah pred tem, da bi država ne mogla več nadzorovati kriminala oz. sovražnih dejavnosti proti njej sami. Ker samozaščitno ravnanje vključuje med drugim tudi tehnike, ki morebitnemu nadzorovalcu, tako nezakonitemu kakor tudi zakonitemu, izjemno otežijo oziroma onemogočijo nadzorovanje, je vprašanje, ali naj ima država zgolj *možnost,* da posameznike nadzoruje, ali pa naj ima *absolutno pravico* do njihovega nadzorovanja. Glede tega si v slovenski pravni ureditvi velja zapomniti dve določbi *zakona o kazenskem postopku*. Prva določba (5. člen) določa, da obdolženec ni dolžan pričati proti sebi ali svojim bližnjim ali priznati krivde. Posledice te določbe za obdolženca, ki je uporabljal šifriranje, pomenijo, da mu v postopku proti njemu ni treba povedati gesel, na podlagi katerih bi preiskovalci lahko odprli zašifrirano sporočilo, ter tako prišli do