behulpzaam zijn door privacygevoelige informatie te markeren of op basis van specifieke bedrijfsregels te onderscheppen. Zo is het voorstelbaar dat, bij het aanleveren van gegevens voor het ELD, de software aan de kant van de ontvangende school bepaalde privacygevoelige informatie alleen ophaalt indien het gaat om een leerling die feitelijk bij de ontvangende school wordt ingeschreven. Indien nog niet vaststaat dat de leerling bij de ontvangende school zal worden ingeschreven, zoals in het geval van een proefplaatsing, zouden deze gegevens dan niet opgehaald worden. De regels die dit onderscheid maken, zouden ook ingebouwd kunnen worden in de centrale waar ELD's verzameld worden.

Dit type voorzieningen is echter ineffectief als de informatie die wordt uitgewisseld is opgeslagen in een structuur waarvan de inhoud niet geautomatiseerd geanalyseerd en verwerkt kan worden. Indien de standaard voor gegevensuitwisseling voorziet in het uitwisselen van digitale bestanden, zoals tekstbestanden, pdf-bestanden of fotobestanden, dan kan privacygevoelige informatie die zich in deze bestanden bevindt niet automatisch gesignaleerd worden. Dit geldt voor gegevensuitwisseling per e-mail, en ook voor gegevensuitwisseling met e-mail-vervangers, zoals XML-'webservices'. Als een school een handelingsplan in Microsoft Word heeft aangeleverd aan het ELD, dan onttrekt de inhoud van het handelingsplan zich aan een geautomatiseerde controle op privacygevoelige informatie. Het meezenden van documenten binnen een XML-bestand vormt onvermijdelijk een 'lek' in de bescherming van de privacy.[206] Omdat in het bestand gegevens kunnen zijn opgenomen die betrekking hebben op andere personen dan de leerling, en de aanleverende school abusievelijk een verkeerd bestand bijgesloten kan hebben, zouden niet alleen gegevens die betrekking hebben op de leerling via dit lek naar buiten kunnen druppelen, maar ook gegevens die betrekking hebben op andere leerlingen of medewerkers of derden.

#### 3.5.3.3.3 De schadelijkheid van pseudo-garanties

Voor wie met inzicht in de wet terugkijkt naar de wijze waarop er gecommuniceerd wordt over privacygevoelige informatie, wordt de schade van pseudo-garanties zichtbaar. Voor zover de WBP geen anachronisme is en het zin heeft de burger te beschermen tegen inbreuken op de privacy, moet als voornaamste risicofactor worden aangemerkt de argeloosheid waarmee heden ten dage met informatie in de rondte wordt geslingerd.[207] Door naar een

[206] De onderzoeker heeft de projectgroep ELD op dit lek gewezen. Cf. e-mail onderzoeker aan ELD-projectgroep, 20 mei 2009, 21:31. De ELD-projectgroep heeft aangegeven dat er concept-reactie van de jurist hierover is opgesteld die geformaliseerd zou worden. Cf. e-mail ELD-projectgroep aan onderzoeker, 24 augustus 2009, 15:10. Door de gestelde einddatum voor de redactie van die boek kon deze eventuele formele reactie van de ELD-projectgroep niet in deze analyse meegenomen worden.

[207] Volgens velen is de intentie achter de WBP - de burger beschermen tegen misbruik van prive-informatie - achterhaald nu bijna iedereen een GSM op zak heeft waarmee men permanent gevolgd zou kunnen worden en de argeloosheid waarmee jan en alleman informatie verzamelt, reproduceert en verspreidt via kanalen die men zelf niet kan controleren. Dit is in de context van